ESET SMART SECURITY 5

Guide de l’utilisateur

(versions 5.2 et ultérieures)

Microsoft® Windows® 8 / 7 / Vista / XP / 2000 / Home Server

Cliquez ici pour télécharger la dernière version de ce document.



ESET **SMART SECURITY**

Assistance clientèle internationale : www.eset.com/support

RÉV. 12/10/2012

Table des

1. ESET Smart Security

ESET Smart Security 5 représente une nouvelle approche de sécurité informatique véritablement intégrée. La dernière version du moteur d'analyse ThreatSense®, associée à un pare-feu personnel et à des modules antispam personnalisés, garantissent la sécurité de votre ordinateur avec grande précision et rapidité. Le résultat est un système intelligent et constamment en alerte, qui protège votre ordinateur des attaques et des programmes malveillants.

ESET Smart Security 5 est une solution de sécurité complète, fruit d'un long travail et d'efforts continus pour parvenir à une protection maximale avec une empreinte minimale sur le système. Des technologies avancées basées sur l'intelligence artificielle sont capables de faire barrage de manière proactive à l'infiltration de virus, de logiciels espions, de chevaux de Troie, de vers, de logiciels publicitaires, de rootkits et d'autres attaques provenant d'Internet, sans réduire les performances ni perturber votre ordinateur.

1.1 Nouveautés

Contrôle parental

Contrôle parental permet de bloquer les sites dont le contenu peut être choquant. En outre, les parents peuvent interdire l'accès à plus de 20 catégories de sites Web prédéfinies. Cet outil empêche les enfants et les jeunes adultes d'accéder à des pages au contenu inapproprié ou nuisible.

HIPS

Le système HIPS (Host Intrusion Prevention System) protège votre système des logiciels malveillants et de toute activité non souhaitée qui pourrait avoir une incidence sur votre ordinateur. Il utilise l'analyse avancée des comportements, associée aux fonctionnalités de détection du filtre réseau qui surveille les processus en cours, les fichiers et les clés de registre, afin de bloquer activement et d'empêcher toute tentative de ce type.

Antispam amélioré

Le module antispam intégré dans ESET Smart Security a été optimisé pour offrir une meilleure précision de détection.

Rejoignez le réseau ESET Live Grid

Fondée sur le système d'avertissement anticipé avancé ThreatSense.Net, la fonctionnalité ESET Live Grid est conçue pour renforcer la sécurité de votre ordinateur. Elle surveille en permanence les programmes et processus en cours d'exécution sur votre système à partir des dernières informations collectées auprès de millions d'utilisateurs ESET à travers le monde. En outre, les analyses de votre système gagnent en rapidité et en précision à mesure du développement de la base de données ESET Live Grid. Cela nous permet d'offrir à tous nos utilisateurs une meilleure protection proactive et des analyses plus rapides. Nous vous recommandons d'activer cette fonctionnalité et vous remercions de votre soutien.

Contrôle des supports amovibles

ESET Smart Security permet de contrôler les supports amovibles (CD/DVD/USB/...). Ce module permet d'analyser, de bloquer ou d'ajuster les filtres étendus/autorisations, et de contrôler la façon dont l'utilisateur peut accéder à un périphérique pour l'utiliser. Ce procédé peut être utile si l'administrateur souhaite empêcher les utilisateurs d'insérer des supports amovibles stockant du contenu non sollicité.

Mode joueur

Mode joueur s'adresse aux utilisateurs qui ne veulent pas être interrompus et dérangés par l'ouverture de fenêtres ou qui souhaitent minimiser l'utilisation du processeur. Mode joueur peut également être utilisé comme mode de présentation, lorsque la présentation ne peut pas être interrompue par l'activité antivirus. Lorsque cette fonctionnalité est activée, toutes les fenêtres contextuelles sont désactivées et l'activité du planificateur est complètement arrêtée. La protection du système continue à fonctionner en arrière-plan, mais n'exige aucune interaction de la part de l'utilisateur.

Rechercher les mises à jour du produit

Outre les mises à jour de la base des signatures de virus et des modules de programme, ESET Smart Security peut également être configuré pour vérifier régulièrement la dernière version du produit. Au cours de l'installation, si vous utilisez un package ancien, vous pouvez choisir de télécharger et d'installer automatiquement la dernière version de ESET Smart Security.

Nouvelle conception

La fenêtre principale de ESET Smart Security a été entièrement repensée et la configuration avancée plus intuitive simplifie la navigation.

1.2 Configuration système

Pour garantir le fonctionnement correct d'ESET Smart Security, le système doit répondre à la configuration suivante :

Microsoft® Windows® 2000, XP

400 MHz 32 bits (x86)/64 bits (x64)
128 Mo de RAM de mémoire système
320 Mo d'espace disponible
Super VGA (800 x 600)

Microsoft® Windows® 8, 7, Vista, Home Server

1 GHz 32 bits (x86)/64 bits (x64)
512 Mo de RAM de mémoire système
320 Mo d'espace disponible
Super VGA (800 x 600)

1.3 Prévention

Lorsque vous travaillez sur votre ordinateur et particulièrement lorsque vous surfez sur Internet, gardez toujours à l'esprit qu'aucun antivirus au monde ne peut complètement éliminer le risque lié aux infiltrations et. attaques. Pour bénéficier d'une protection maximale, il est essentiel d'utiliser le système antivirus correctement et de respecter quelques règles essentielles.

Mettre à jour régulièrement

Selon les statistiques de ESET Live Grid, des milliers de nouvelles infiltrations sont créées chaque jour pour contourner les dispositifs de sécurité existants et servir leurs auteurs, aux dépens des autres utilisateurs. Les spécialistes du laboratoire d'ESET analysent ces menaces chaque jour et conçoivent des mises à jour visant à améliorer en continu le niveau de protection des utilisateurs du programme antivirus. Une mise à jour mal configurée altère l'efficacité du programme. Pour plus d'informations sur la procédure de configuration des mises à jour, reportez-vous au chapitre Configuration des mises à jour.

Télécharger les patchs de sécurité

Les auteurs de programmes malveillants préfèrent exploiter diverses failles du système pour assurer une meilleure propagation du code malveillant. C'est pourquoi les sociétés qui commercialisent des logiciels recherchent activement l'apparition de nouvelles failles dans leurs applications pour concevoir les mises à jour de sécurité permettant d'éliminer régulièrement les menaces potentielles. Il est important de télécharger ces mises à jour de sécurité au moment de leur sortie. Ces mises à jour concernent par exemple le système d'exploitation de Windows ou le navigateur Internet Explorer.

Sauvegarder les données importantes

Les concepteurs de programmes malveillants ne se soucient généralement pas des besoins des utilisateurs et l'activité de leurs programmes entraîne souvent un dysfonctionnement total du système d'exploitation et des dommages importants au niveau des données. Il est important de sauvegarder régulièrement vos données importantes et sensibles sur une source externe, telle que DVD ou disque dur externe. Ces précautions permettront de récupérer vos données beaucoup plus facilement et rapidement en cas de défaillance du système.

Rechercher régulièrement les virus sur votre ordinateur

Une analyse automatique régulière de votre ordinateur avec les paramètres adéquats peut permettre de supprimer les infiltrations qui ont pu être ignorées par d'anciennes mises à jour de signatures de virus.

Suivre les règles de sécurité de base

Cette règle est la plus utile et la plus efficace de toutes : soyez toujours prudent. Actuellement, de nombreuses infiltrations nécessitent l'intervention de l'utilisateur pour être exécutées et propagées. Si vous êtes prudent lorsque vous ouvrez de nouveaux fichiers, vous éviterez de perdre un temps et une énergie considérable à nettoyer votre ordinateur. Respectez les règles suivantes :

- Ne consultez pas les sites Web suspects comportant de nombreuses fenêtres publicitaires et annonces clignotantes.
- Soyez vigilant lorsque vous installez des logiciels gratuits, des packs codec, etc. N'utilisez que des programmes sécurisés et ne visitez que les sites Web sécurisés.
- Soyez prudent lorsque vous ouvrez les pièces jointes des messages électroniques, en particulier celles de messages provenant de mailing ou d'expéditeurs inconnus.
- N'utilisez pas de compte Administrateur pour le travail de tous les jours sur votre ordinateur.

2. Installation

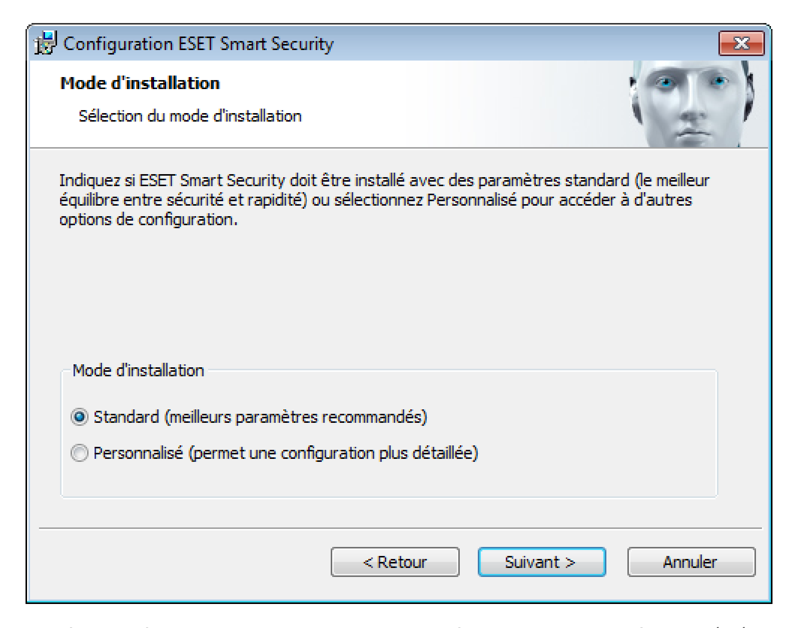
Lancez le programme d'installation ; l'assistant d'installation vous guide tout au long du processus de configuration.

Important : Assurez-vous qu'aucun autre programme antivirus n'est installé sur votre ordinateur. Si plusieurs solutions antivirus sont installées sur un même ordinateur, elles risquent de provoquer des conflits. Nous recommandons de désinstaller tout autre antivirus de votre système. Reportez-vous à notre article de la base de connaissances pour obtenir une liste des outils de désinstallation des logiciels antivirus courants (disponible en anglais et dans plusieurs autres langues).

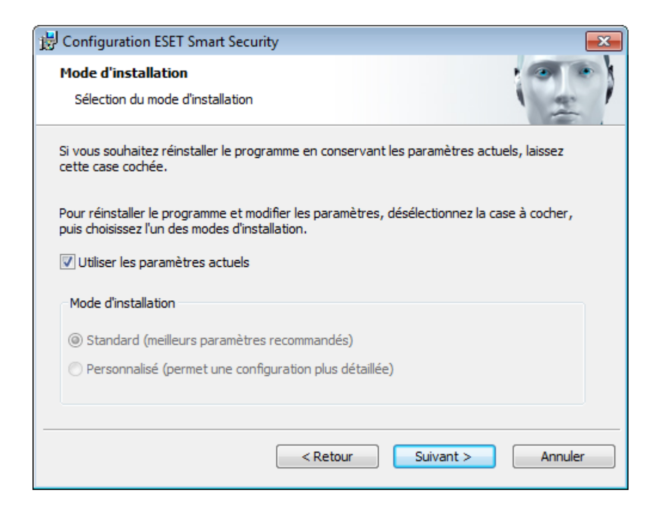


Tout d'abord, le programme vérifie si une version plus récente de ESET Smart Security est disponible. S'il existe une version plus récente, vous en êtes informé au cours de la première étape du processus d'installation. Si vous sélectionnez l'option de **téléchargement et d'installation de la nouvelle version**, la nouvelle version est téléchargée et l'installation se poursuit. Le contrat de licence de l'utilisateur final (CLUF) apparaît à l'étape suivante. Veuillez en prendre connaissance, puis cliquez sur **Accepter** pour confirmer que vous acceptez les clauses du contrat de licence de l'utilisateur final. L'installation se poursuit ensuite selon l'un des deux scénarios suivants :

1. Si vous installez ESET Smart Security sur un ordinateur pour la première fois, la fenêtre ci-dessous apparaît lorsque vous acceptez le **contrat de licence de l'utilisateur final**. Vous avez le choix entre une installation standard ou personnalisée et accédez aux options correspondantes.



2. Si vous installez ESET Smart Security sur une version précédente du logiciel, la fenêtre ci-dessous vous permet de choisir d'utiliser les paramètres actuels du programme pour la nouvelle installation ; ou, si vous décochez l'option **Utiliser les paramètres actuels**, de choisir entre les deux modes d'installation précités.



2.1 Installation standard

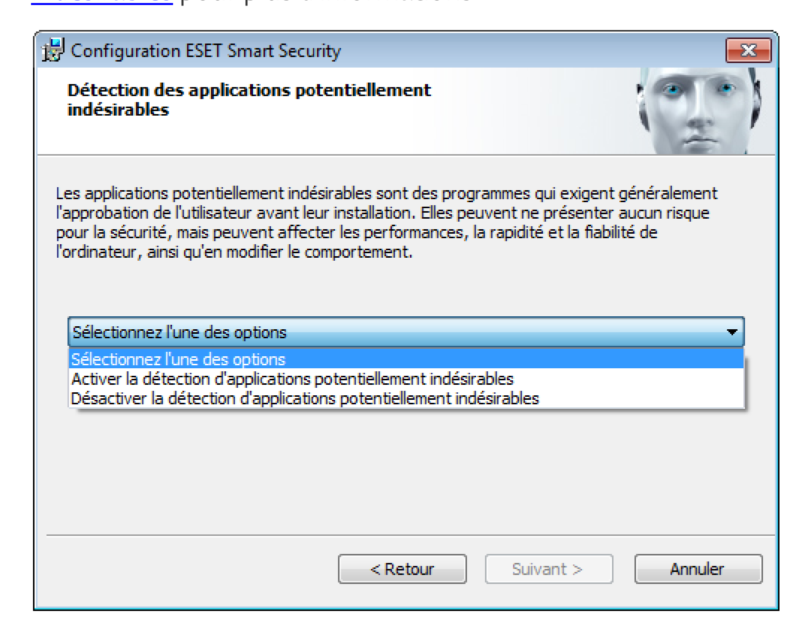
Le mode d'installation standard comprend des options de configuration qui correspondent à la plupart des utilisateurs. Ces paramètres offrent un excellent système de sécurité très facile à utiliser et des performances système très élevées. Le mode d'installation standard est l'option par défaut qui est recommandée si vous n'avez pas d'exigence particulière pour certains paramètres.

Après avoir sélectionné le mode d'installation et cliqué sur **Suivant**, vous êtes invité à configurer ESET Live Grid. Le système ESET Live Grid contribue à garantir qu'ESET est informé immédiatement et en continu des nouvelles infiltrations, afin de protéger ses clients. Le système permet de soumettre les nouvelles menaces au laboratoire d'ESET, où elles sont analysées, traitées, puis ajoutées à la base des signatures de virus.

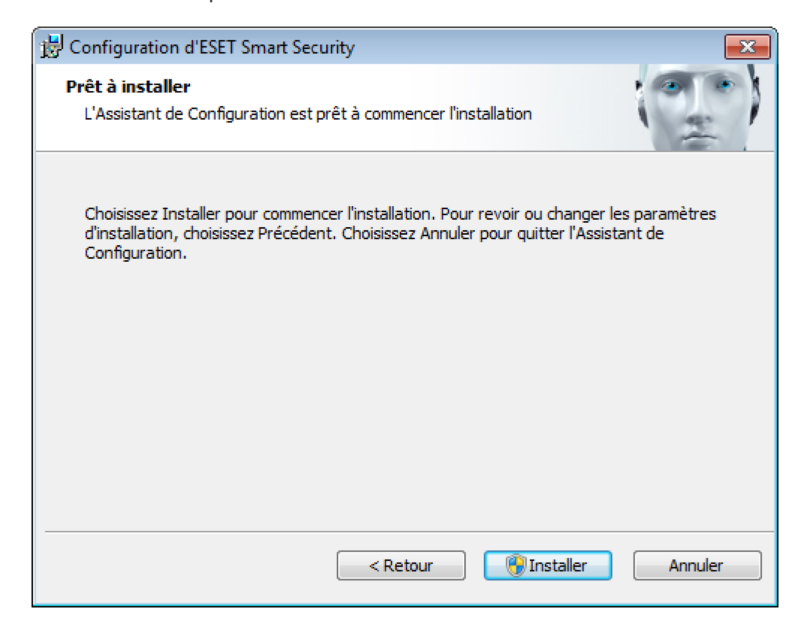


Par défaut, l'option **J'accepte de participer à ESET Live Grid** est sélectionnée et active cette fonctionnalité.

L'étape suivante de l'installation consiste à configurer la détection des applications potentiellement indésirables. Les applications potentiellement indésirables ne sont pas nécessairement malveillantes, mais peuvent avoir une incidence négative sur le comportement du système d'exploitation. Reportez-vous au chapitre Applications potentiellement indésirables pour plus d'informations.



La dernière étape de l'installation standard consiste à confirmer l'installation en cliquant sur le bouton **Installer**.



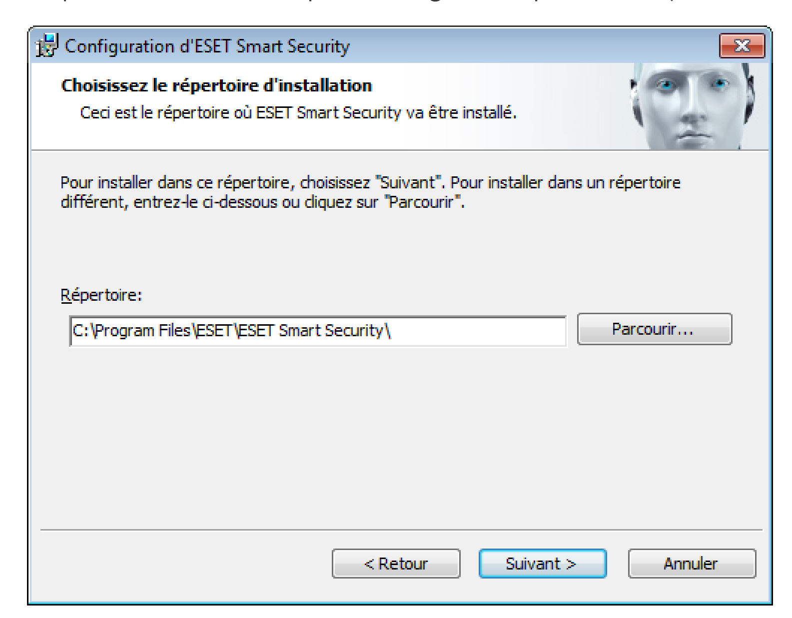
2.2 Installation personnalisée

Le mode d'installation personnalisée est destiné à des utilisateurs qui ont une certaine expérience de l'optimisation de programmes, et qui veulent modifier les paramètres avancés pendant l'installation.

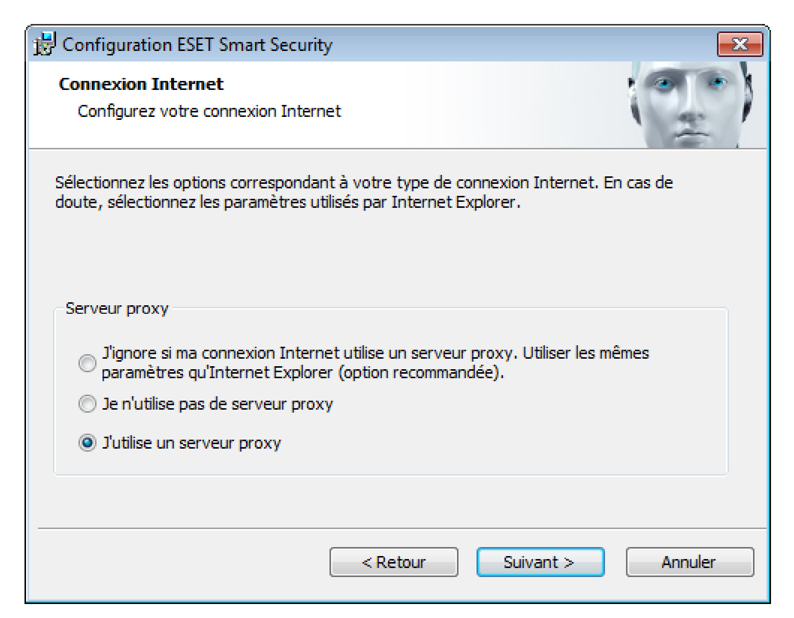
Après avoir sélectionné le mode d'installation et cliqué sur **Suivant**, vous êtes invité à sélectionner un emplacement de destination pour l'installation. Par défaut, le système installe le programme dans le répertoire suivant :

C:*Program Files\ESET\ESET Smart Security*

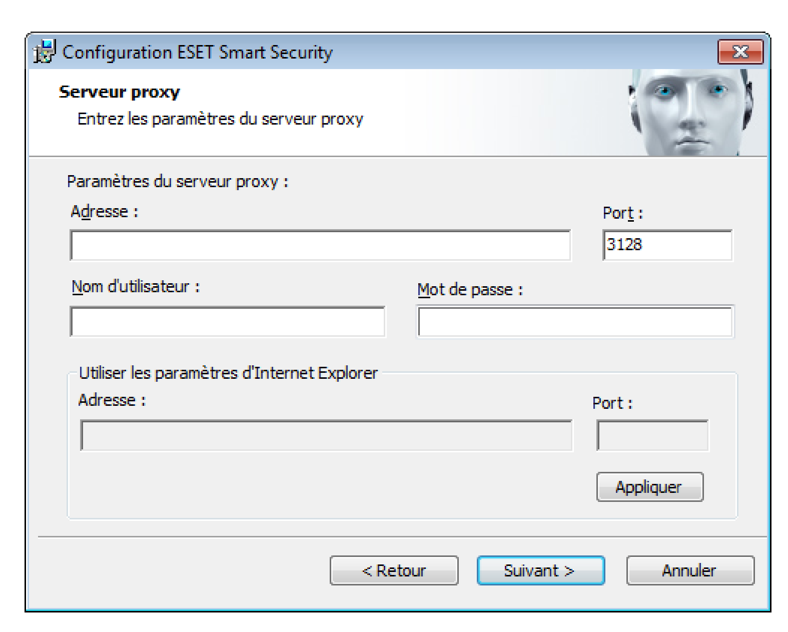
Cliquez sur **Parcourir...** pour changer d'emplacement (non recommandé).



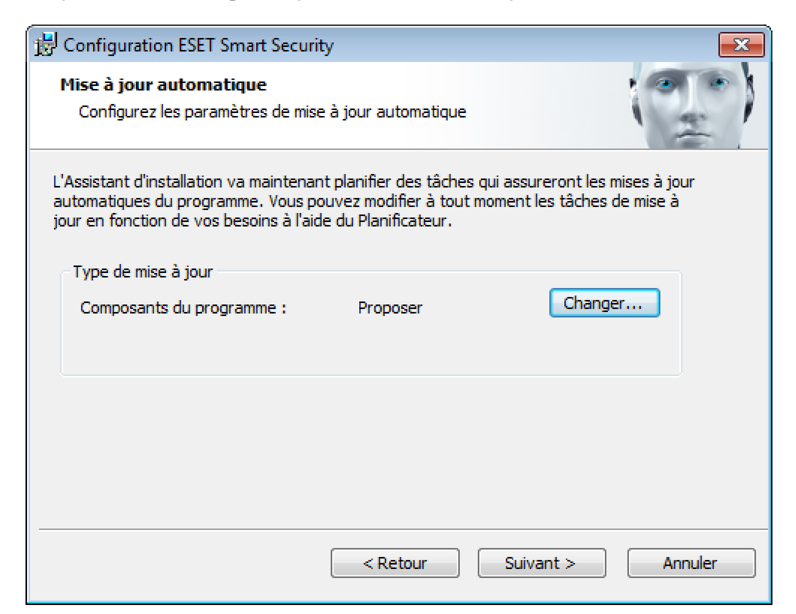
Cliquez sur **Suivant** et continuez avec la configuration de votre connexion Internet. Si vous utilisez un serveur proxy, ce dernier doit être configuré correctement pour que les mises à jour des signatures de virus fonctionnent. Si vous ne savez pas exactement si vous utilisez ou non un serveur proxy pour la connexion à Internet, sélectionnez **Je ne sais pas si ma connexion Internet utilise un serveur proxy. Utiliser les mêmes paramètres qu'Internet Explorer (option recommandée).** et cliquez sur **Suivant**. Si vous n'utilisez pas de serveur proxy, sélectionnez l'option **Je n'utilise pas de serveur proxy**.



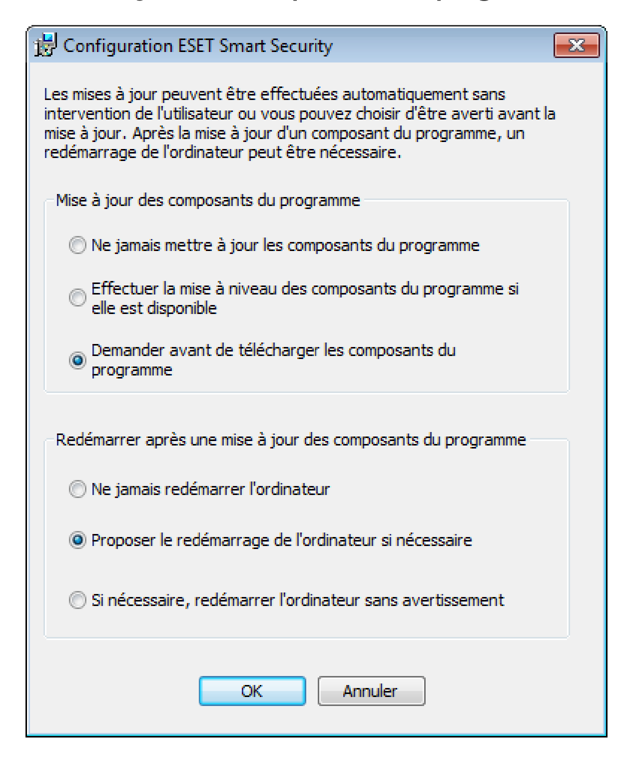
Pour configurer les paramètres du serveur proxy, sélectionnez l'option **J'utilise un serveur proxy** et cliquez sur **Suivant**. Entrez l'adresse IP ou l'adresse URL de votre serveur proxy dans le champ **Adresse**. Dans le champ **Port**, spécifiez le port sur lequel le serveur proxy accepte les connexions (3128 par défaut). Si le serveur proxy exige une authentification, saisissez un **nom d'utilisateur** et un **mot de passe** pour accorder l'accès au serveur proxy. Les paramètres du serveur proxy peuvent être copiés depuis Internet Explorer. Pour ce faire, cliquez sur le bouton **Appliquer** et confirmez la sélection.



Cette étape d'installation permet d'indiquer la façon dont le système gère les mises à jour automatiques du programme. Cliquez sur **Changer...** pour accéder aux paramètres avancés.

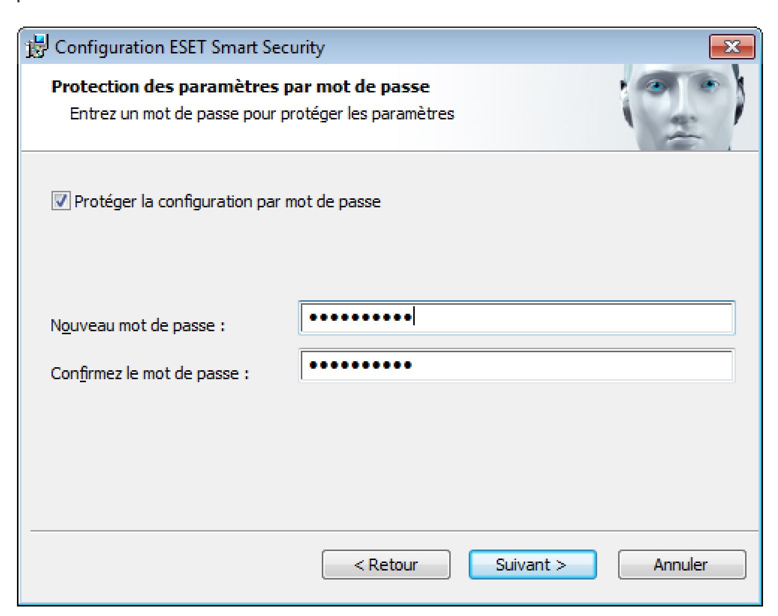


Si vous ne voulez pas que les composants du programme soient mis à jour, sélectionnez l'option **Ne jamais mettre à jour les composants du programme**. Sélectionnez l'option **Demander avant de télécharger les composants du programme** pour afficher une fenêtre de confirmation chaque fois que le système essaie de télécharger les composants du programme. Pour télécharger les mises à niveau des composants du programme, sélectionnez l'option **Toujours mettre à jour les composants du programme**.



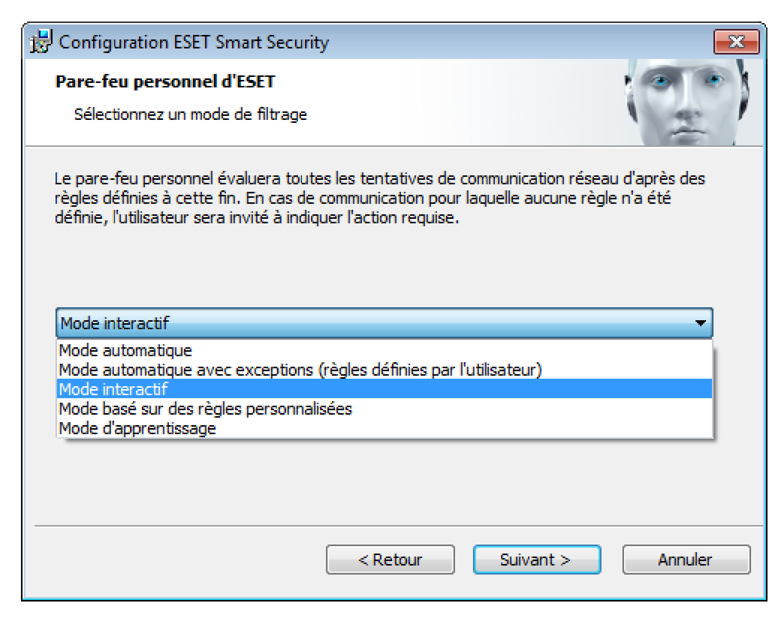
REMARQUE : le redémarrage du système est généralement nécessaire après la mise à jour des composants du programme. il est recommandé de sélectionner l'option **Si nécessaire, redémarrer l'ordinateur sans avertissement**.

La fenêtre suivante de l'installation permet d'indiquer un mot de passe afin de protéger les paramètres du programme. Sélectionnez l'option **Protéger la configuration par mot de passe** et entrez votre mot de passe dans les champs **Nouveau mot de passe** et **Confirmer le nouveau mot de passe**. Ce mot de passe vous sera demandé pour modifier les paramètres de ESET Smart Security ou pour y accéder. Si les deux mots de passe correspondent, cliquez sur **Suivant** pour continuer.



Les étapes d'installation suivantes, **ESET Live Grid** et **Détection des applications potentiellement indésirables** sont traitées de la même manière que dans le mode d'installation standard (reportez-vous à Installation standard).

Sélectionnez ensuite un mode de filtrage pour le pare-feu personnel ESET. Cinq modes de filtrage sont disponibles pour le pare-feu personnel ESET Smart Security. Le comportement du pare-feu change en fonction du mode sélectionné. Les modes de filtrage affectent également le niveau d'interaction de l'utilisateur.



Cliquez sur **Installer** dans la fenêtre **Prêt à installer** pour terminer l'installation. Une fois l'installation terminée, vous êtes invité à activer le produit. Reportez-vous à l'installation standard pour plus d'informations sur l'activation du produit.

2.3 Activation du produit

Une fois l'installation terminée, vous êtes invité à activer le produit.

Il existe plusieurs options d'activation. Certains scénarios d'activation proposés dans la fenêtre d'activation peuvent varier en fonction du pays et selon le mode de distribution du fichier d'installation (CD/DVD, page Web ESET, etc.).

Si vous disposez d'une version emballée, achetée au détail, du produit , sélectionnez l'option **Utiliser une clé d'activation**. Cette clé d'activation se trouve généralement à l'intérieur ou au dos de l'emballage du produit. Vous devez entrer la clé d'activation exactement comme elle est indiquée.

Si vous avez reçu un nom d'utilisateur et un mot de passe, sélectionnez l'option **Activer à l'aide d'un nom d'utilisateur et d'un mot de passe**, puis entrez vos informations d'identification dans les champs appropriés.

Si vous souhaitez évaluer ESET Smart Security avant d'en faire l'acquisition, sélectionnez l'option **Activer la licence d'essai**. Indiquez votre adresse électronique et le pays dans lequel vous résidez pour activer ESET Smart Security pendant une période limitée. Votre licence de test sera envoyée à cette adresse. Les licences de test ne peuvent être activées qu'une seule fois par client.

Si vous n'avez pas de licence et souhaitez en acheter une, cliquez sur l'option **Acheter une licence**. Cette opération vous redirigera vers le site Web de votre distributeur ESET local.

Sélectionnez l'option **Activer ultérieurement** si vous souhaitez évaluer rapidement notre produit avant de l'activer ou si vous souhaitez l'activer ultérieurement.

Vous pouvez activer votre copie de ESET Smart Security directement à partir du programme. Cliquez sur l'icône Menu du programme située dans l'angle supérieur droit ou cliquez à l'aide du bouton droit de la souris sur l'icône ESET Smart Security de la barre des tâches, puis cliquez sur et sélectionnez **Activation de produit...** dans le menu.

2.4 Saisie du nom d'utilisateur et du mot de passe

Le programme doit être mis à jour automatiquement pour assurer un fonctionnement optimal. Ce téléchargement n'est possible que si le nom d'utilisateur et le mot de passe sont saisis dans l'option **Configuration de la mise à jour**.

Si vous n'avez pas entré votre nom d'utilisateur et votre mot de passe lors de l'installation, vous pouvez le faire maintenant. Dans la fenêtre principale, cliquez sur **Mettre à jour** et **Activation du produit...**, puis entrez dans la fenêtre d'activation du produit les informations de la licence que vous avez reçues avec votre produit de sécurité ESET.

Lors de la saisie de votre **nom d'utilisateur** et de votre **mot de passe**, il est important de respecter scrupuleusement leur forme :

- Le nom d'utilisateur et le mot de passe font la distinction entre les majuscules et les minuscules, et le tiret dans le nom d'utilisateur est obligatoire.
- Le mot de passe se compose de dix caractères, tous en minuscules.
- Nous n'utilisons pas la lettre « L » dans les mots de passe (utilisez le numéro un (1) à la place).
- Le « O » est le chiffre zéro et le « o » est la lettre minuscule o.

Il est recommandé de copier et de coller les données à partir du message d'enregistrement.

2.5 Mise à niveau vers une nouvelle version

Les nouvelles versions de ESET Smart Security offrent des améliorations ou apportent des solutions aux problèmes que les mises à jour automatiques des modules ne peuvent pas résoudre. La mise à niveau vers une nouvelle version peut s'effectuer de différentes manières :

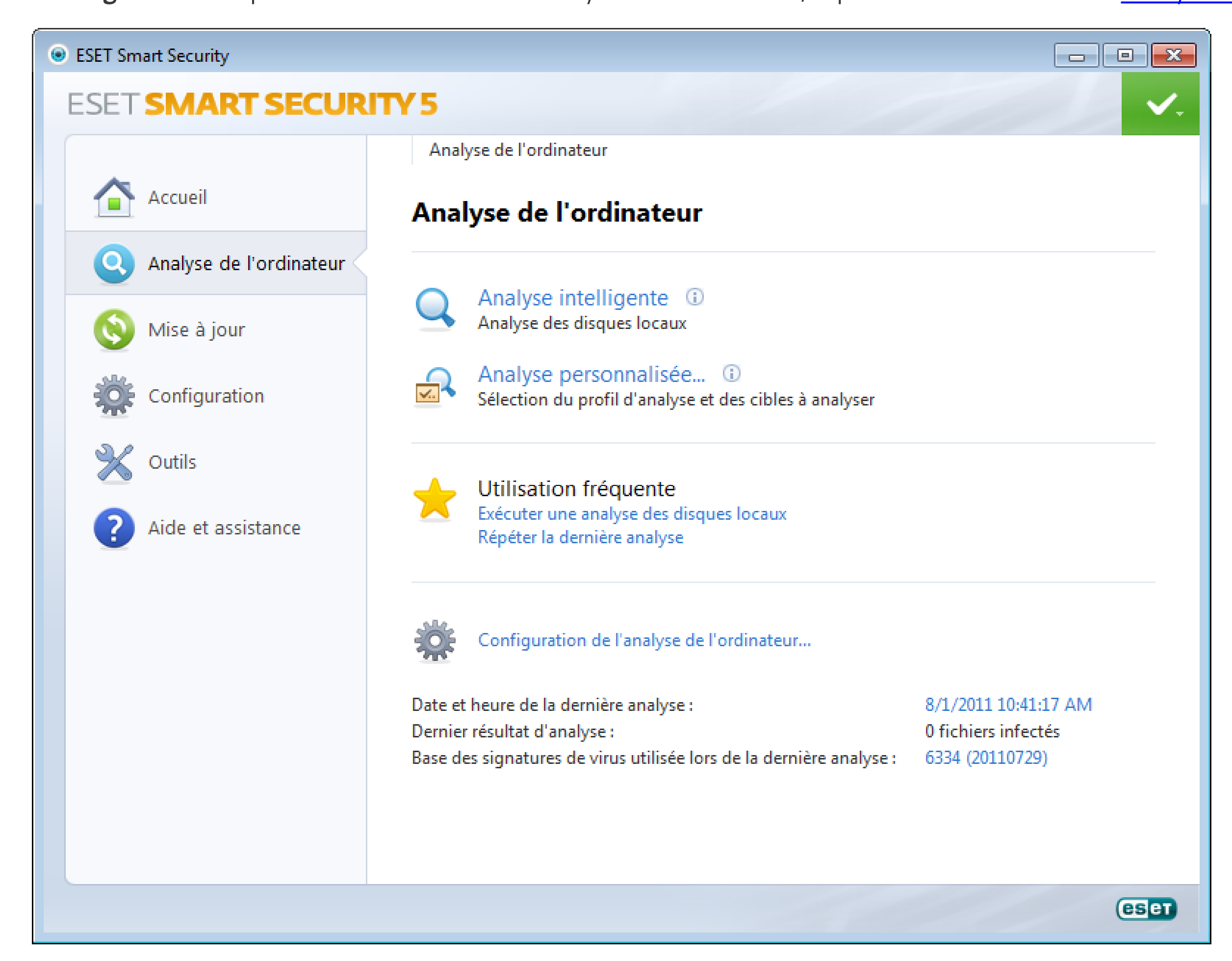
1. Automatiquement, par l'intermédiaire d'une mise à jour du programme.
   Les mises à niveau du programme sont distribuées à tous les utilisateurs et peuvent avoir un impact sur certaines configurations système. Elles sont par conséquent mises à disposition après de longues périodes de test afin que leur fonctionnement correct soit garanti sur toutes les configurations système. Pour effectuer la mise à niveau vers une nouvelle version dès que celle-ci est disponible, utilisez l'une des méthodes ci-dessous.

2. Manuellement, en téléchargeant la nouvelle version et en l'installant sur l'installation précédente.
   Au début de l'installation, vous pouvez choisir de conserver les paramètres du programme en cochant la case **Utiliser les paramètres actuels**.

3. Manuellement, dans la fenêtre principale du programme, en cliquant sur l'option **d'installation/de vérification** dans **Mettre à jour** > **Version disponible de ESET Smart Security**.

2.6 Analyse d'ordinateur

Après l'installation d'ESET Smart Security, vous devez effectuer une analyse de l'ordinateur afin de rechercher tout code malveillant éventuel. Dans la fenêtre principale du programme, cliquez sur **Analyse de l'ordinateur**, puis sur **Analyse intelligente**. Pour plus d'informations sur l'analyse de l'ordinateur, reportez-vous à la section Analyse de l'ordinateur.



3. Guide du débutant

Ce chapitre donne un premier aperçu d'ESET Smart Security et de ses paramètres de base.

3.1 Présentation de l'interface utilisateur

La fenêtre principale d'ESET Smart Security est divisée en deux sections principales. La fenêtre principale de droite affiche les informations correspondant à l'option sélectionnée dans le menu principal à gauche.

Voici une description des options disponibles dans le menu principal :

Accueil - Fournit des informations sur l'état de protection de ESET Smart Security.

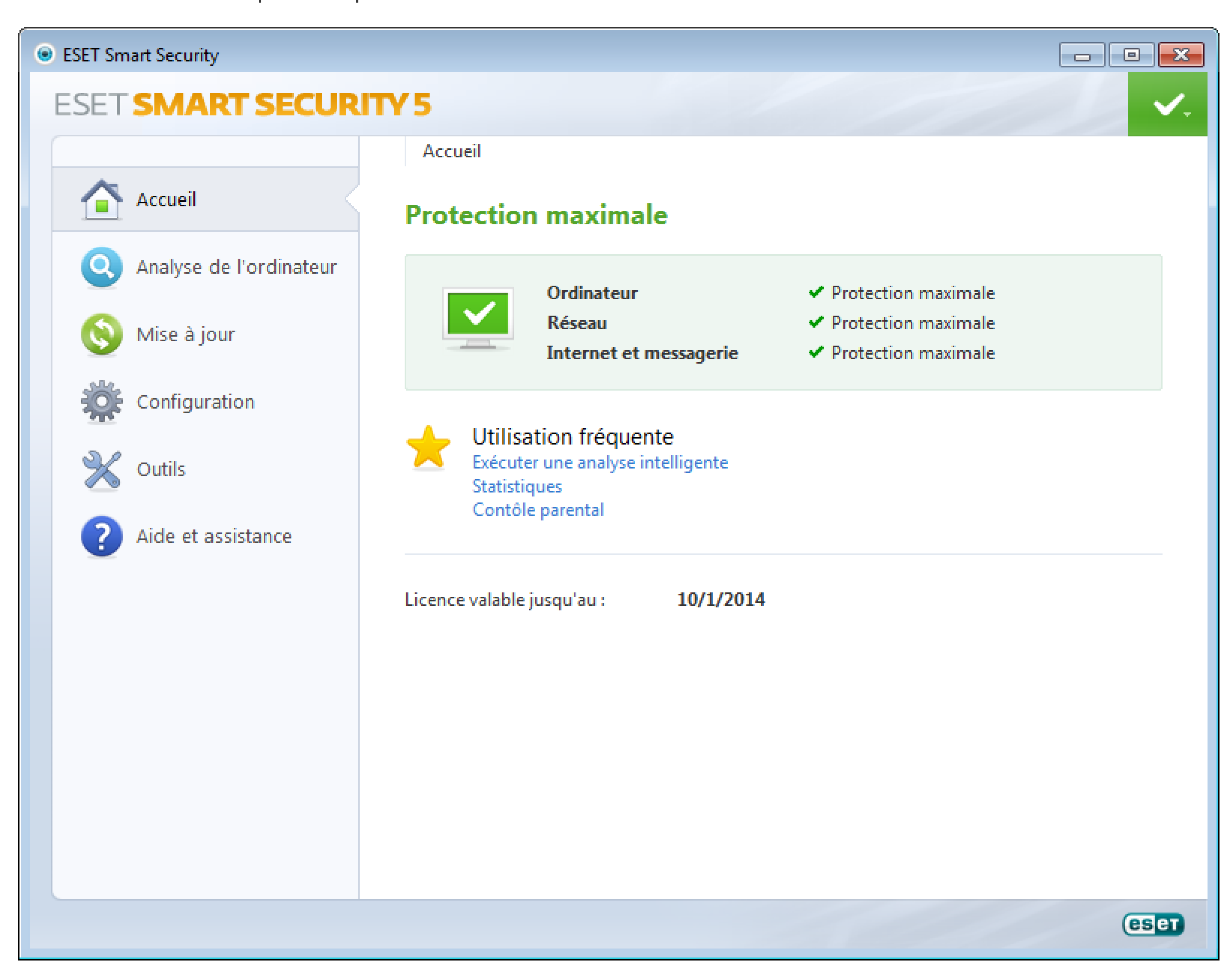
Analyse de l'ordinateur - Cette option permet de configurer et de lancer l'analyse intelligente ou l'analyse personnalisée.

Mettre à jour - Affiche des informations sur les mises à jour de la base des signatures de virus.

Configuration - Sélectionnez cette option pour ajuster le niveau de sécurité de votre ordinateur, d'Internet et de la messagerie, du réseau et de Contrôle parental .

Outils - Permet d'accéder aux fichiers journaux, aux statistiques de protection, à la surveillance de l'activité, aux processus en cours, aux connexions réseau, au planificateur, à la quarantaine, à ESET SysInspector et à ESET SysRescue.

Aide et assistance - Permet d'accéder aux fichiers d'aide, à la Base de connaissances ESET, et aux liens nécessaires à l'ouverture d'une requête auprès du service client.

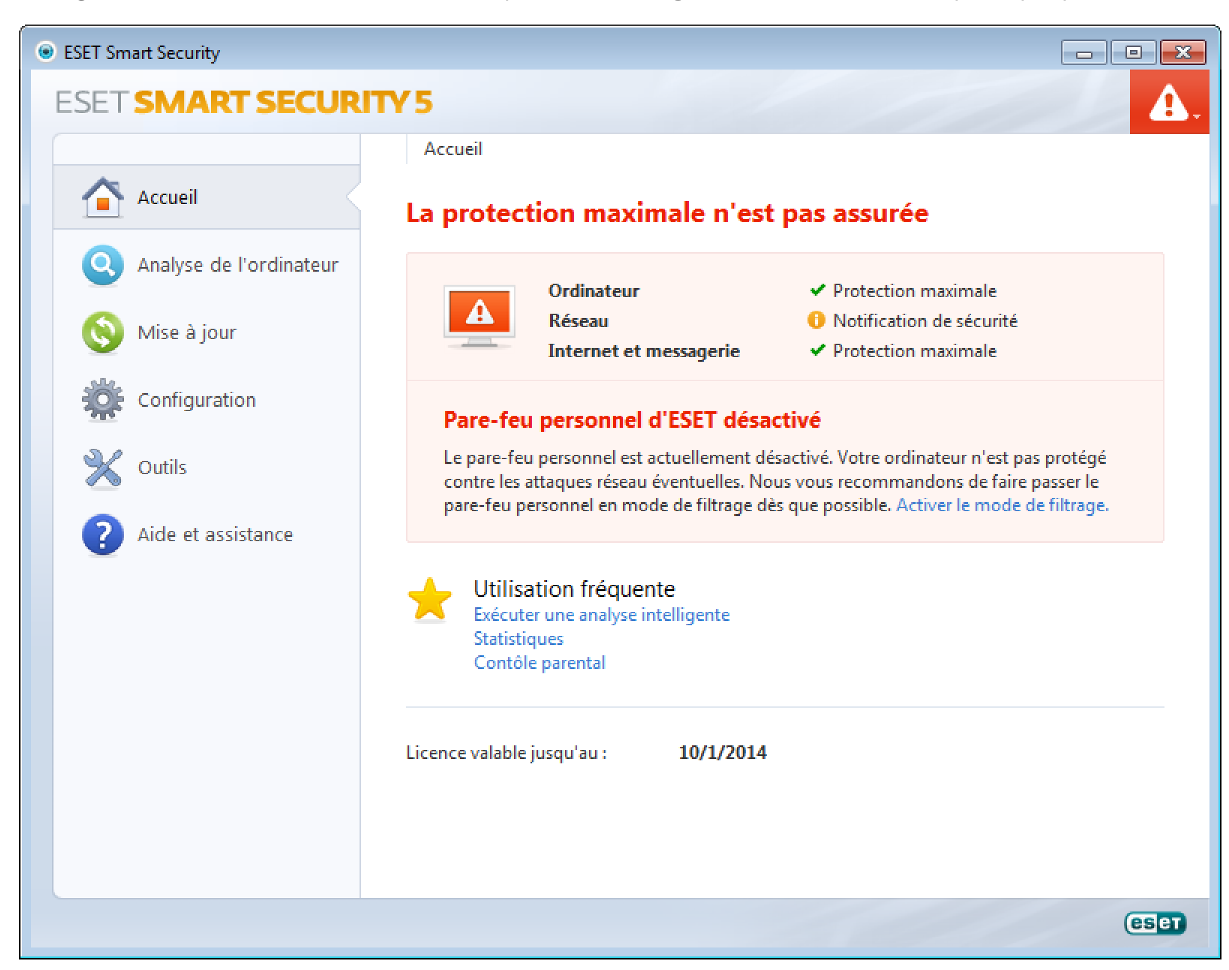


L'écran **Accueil** vous informe sur le niveau actuel de sécurité et de protection de l'ordinateur. L'icône verte d'état **Protection maximale** indique qu'une protection maximale est assurée.

La fenêtre d'état affiche également les fonctionnalités utilisées fréquemment dans ESET Smart Security. La date d'expiration du programme figure également ici.

3.2 Que faire lorsque le programme ne fonctionne pas correctement ?

Une coche verte s'affiche en regard de chaque module activé et fonctionnant correctement. Dans le cas contraire, un point d'exclamation rouge ou orange s'affiche. Des informations supplémentaires sur le module s'affichent dans la partie supérieure de la fenêtre. Une suggestion de solution pour corriger le module est également affichée. Pour changer l'état des différents modules, cliquez sur **Configuration** dans le menu principal puis sur le module souhaité.



L'icône rouge signale des problèmes critiques ; la protection maximale de votre ordinateur n'est pas assurée. Les raisons possibles sont les suivantes :

- la protection en temps réel du système de fichiers est désactivée ;
- le pare-feu personnel est désactivé ;
- la base des signatures de virus est obsolète ,
- le produit n'est pas activé ;
- la licence du produit est expirée.

L'icône orange indique que l'accès Web ou la protection du client de messagerie est désactivé, qu'il y a un problème de mise à jour de programme (la base des signatures de virus est obsolète et ne peut pas être mise à jour) ou que la licence approche de sa date d'expiration.

Produit non activé - Ce problème est signalé par une icône rouge et une notification de sécurité à côté de l'élément **Ordinateur**. Vous pouvez activer ESET Smart Security depuis le menu du programme à l'aide de l'option **Activation de produit...** Le menu du programme est situé dans l'angle supérieur droit de la fenêtre principale du programme.

Protection antivirus et antispyware désactivée - Ce problème est signalé par une icône rouge et une notification de sécurité à côté de l'élément **Ordinateur**. Vous pouvez réactiver la protection antivirus et antispyware en cliquant sur **Démarrer tous les modules de protection antivirus et antispyware**.

Protection de l'accès au Web et antihameçonnage - Ce problème est signalé par une icône orange et la lettre « i », ainsi que par le statut **Notification de sécurité**. Vous pouvez réactiver la Protection de l'accès au Web et antihameçonnage en cliquant sur la notification de sécurité, puis sur **Activer la protection de l'accès au Web et antihameçonnage**.

Pare-feu personnel d'ESET désactivé - Ce problème est signalé par une icône rouge et une notification de sécurité à côté de l'élément **Réseau**. Vous pouvez réactiver la protection réseau en cliquant sur **Activer le mode de filtrage**.

Votre licence va arriver prochainement à expiration - Cette information est donnée par l'icône d'état de protection qui affiche un point d'exclamation. Après l'expiration de la licence, le programme ne peut plus se mettre à jour et l'icône d'état de la protection devient rouge.

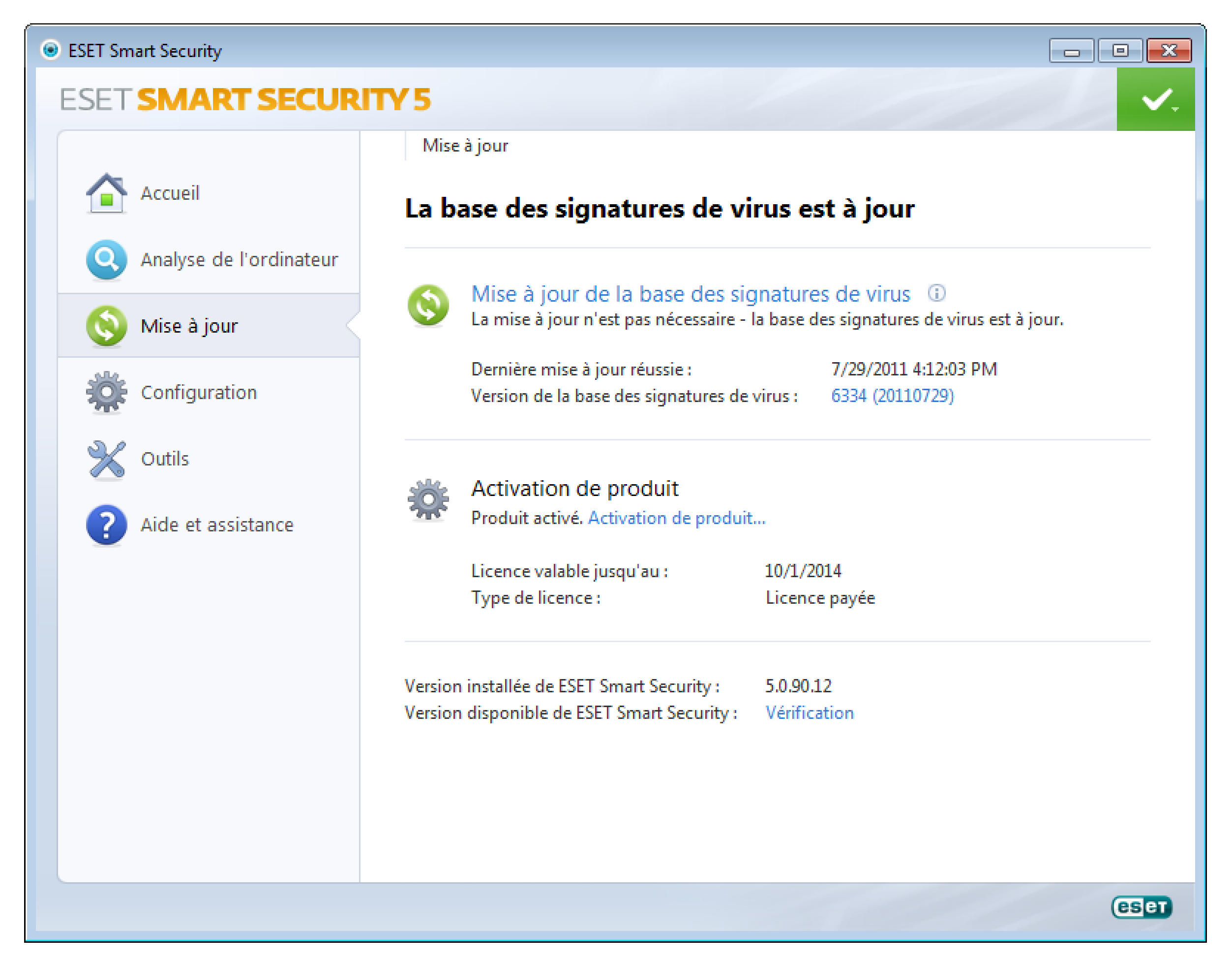
Licence arrivée à expiration - Cette information est indiquée par l'icône d'état de la protection qui devient rouge. Le programme ne peut plus effectuer de mise à jour après expiration de la licence. Nous vous recommandons de suivre les instructions de la fenêtre d'alerte pour renouveler la licence.

Si vous ne parvenez pas à résoudre le problème à l'aide des solutions suggérées, cliquez sur **Aide et assistance** pour accéder aux fichiers d'aide ou pour effectuer des recherches dans la Base de connaissances ESET. Si vous avez encore besoin d'aide, vous pouvez soumettre une demande au service client d'ESET. Ce dernier répondra très rapidement à vos questions et vous permettra de trouver une solution.

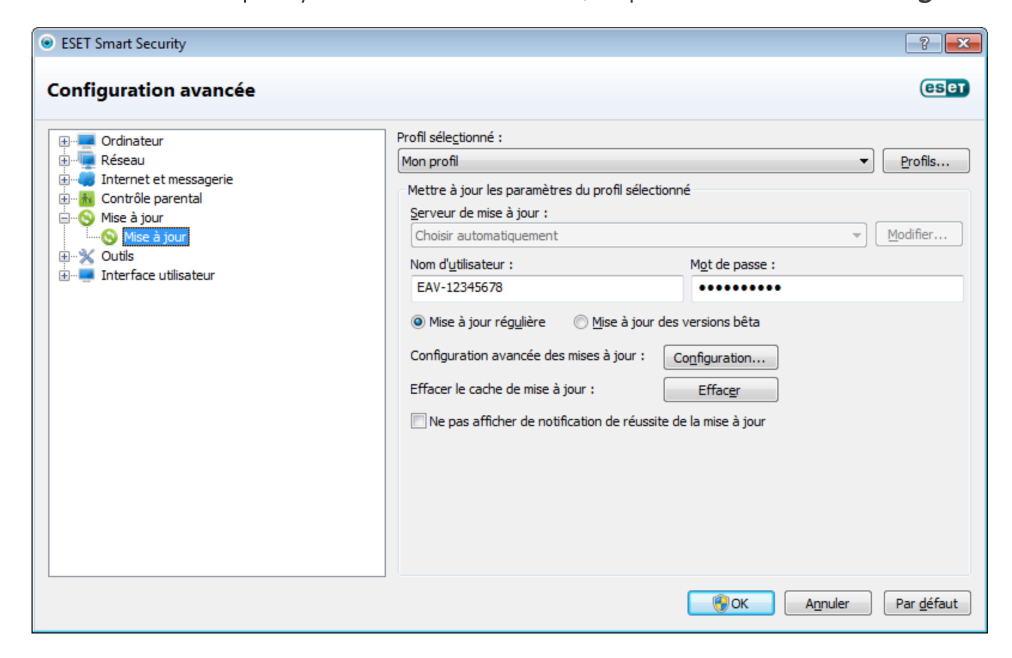
3.3 Configuration des mises à jour

La mise à jour de la base des signatures de virus et celle des composants du programme sont des opérations importantes qui assurent la protection totale contre les attaques des codes malveillants. Il convient donc d'apporter une grande attention à leur configuration et à leur fonctionnement. Dans le menu principal, sélectionnez **Mise à jour** et cliquez sur **Mettre à jour la base des signatures de virus** pour rechercher toute nouvelle mise à jour de la base de données.

Si vous n'avez pas entré votre nom d'utilisateur et votre mot de passe lors du processus d' activation de ESET Smart Security, on vous demandera de le faire maintenant.



La fenêtre Configuration avancée (cliquez sur **Configuration** dans le menu principal et sur **Accéder à la configuration avancée...**, ou appuyez sur la touche F5 de votre clavier) comporte d'autres options de mise à jour. Cliquez sur **Mettre à jour** dans la configuration avancée complète à gauche. Le menu déroulant **Serveur de mise à jour** est grisé et défini sur **Choisir automatiquement**. Pour configurer les options avancées de mise à jour telles que le mode de mise à jour, l'accès au serveur proxy et les connexions LAN, cliquez sur le bouton **Configuration...**



3.4 Configuration de la zone Fiable

La zone Fiable doit être configurée pour que la protection de votre ordinateur dans un réseau soit activée. Vous pouvez autoriser d'autres utilisateurs à accéder à votre ordinateur en configurant la zone Fiable et en autorisant le partage. Cliquez sur **Configuration** > **Réseau** > **Modifier le mode de protection de votre ordinateur sur le réseau...** La fenêtre qui apparaît propose des options qui vous permettent de choisir le mode de protection souhaité de votre ordinateur sur le réseau.

La détection de la zone Fiable s'effectue après l'installation de ESET Smart Security et dès que votre ordinateur se connecte à un nouveau réseau. Il n'est généralement donc pas nécessaire de définir la zone Fiable. Par défaut, la boîte de dialogue s'ouvre à la détection d'une nouvelle zone et vous permet d'en définir le niveau de protection.



Avertissement : une configuration incorrecte de la zone Fiable peut compromettre la sécurité de votre ordinateur.

REMARQUE : par défaut, les postes de travail d'une zone Fiable sont autorisés à accéder aux fichiers et imprimantes partagés, disposent de la communication RPC entrante activée et peuvent bénéficier du partage de bureau à distance.

3.5 Outils du contrôle parental

Si vous avez activité le contrôle parental dans ESET Smart Security, vous devez encore le configurer pour les comptes utilisateur voulus pour que tout fonctionne correctement. Reportez-vous au chapitre Contrôle parental pour la procédure à suivre pour créer des restrictions spécifiques permettant de protéger vos enfants des contenus pouvant être choquants.

4. Utilisation de ESET Smart Security

Les options de configuration d'ESET Smart Security permettent de régler les niveaux de protection de votre ordinateur et du réseau.



Le menu **Configuration** contient les options suivantes :

- **Ordinateur**
- **Réseau**
- **Internet et messagerie**
- **Contrôle parental**

Cliquez sur n'importe quel composant pour régler les paramètres avancés du module de protection correspondant.

La configuration de la protection de l'**ordinateur** permet d'activer ou de désactiver les composants suivants :

- **Protection en temps réel du système de fichiers** - Tous les fichiers ouverts, créés ou exécutés sur l'ordinateur sont analysés pour y rechercher la présence éventuelle de code malveillant.
- **Protection des documents** - La fonctionnalité de protection des documents analyse les documents Microsoft Office avant leur ouverture, ainsi que les fichiers téléchargés automatiquement par Internet Explorer, tels que les éléments Microsoft ActiveX.
- **Blocage de supports amovibles** - Ce module permet d'analyser, de bloquer ou d'ajuster les filtres étendus/autorisations, et de sélectionner la façon dont l'utilisateur peut accéder à un périphérique (CD/DVD/USB...) et l'utiliser.
- **HIPS** - Le système HIPS surveille les événements dans le système d'exploitation et réagit en fonction d'un ensemble de règles personnalisées.
- **Mode joueur** - Active ou désactive le mode joueur. Vous recevez un message d'avertissement (mise en danger potentielle de la sécurité) et la fenêtre principale devient orange lorsque le mode Mode joueur.
- **Anti-Stealth** - Détecte les programmes dangereux tels que les rootkits, qui sont en mesure de se dissimuler du système d'exploitation. Il est impossible de les détecter à l'aide de techniques de test ordinaires.

La section **Réseau** permet d'activer ou de désactiver le **pare-feu personnel**.

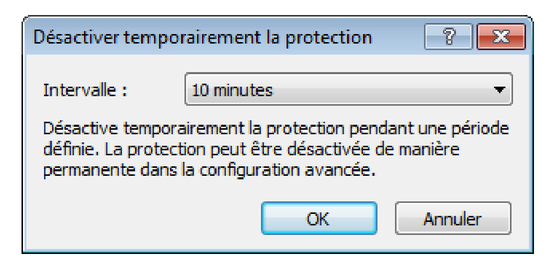
La configuration de la protection **Internet et messagerie** permet d'activer ou de désactiver les composants suivants :

- **Protection de l'accès au Web et antihameçonnage** - Si cette option est activée, tout le trafic HTTP ou HTTPS est analysé à la recherche de codes malveillants.
- **Protection du client de messagerie** - Contrôle les communications reçues via les protocoles POP3 et IMAP.
- **Protection antispam** - La protection antispam recourt à deux méthodes pour détecter les messages non sollicités.

Le contrôle parental permet de bloquer les pages Web dont le contenu peut être choquant. En outre, les parents peuvent interdire l'accès à plus de 20 catégories de sites Web prédéfinies.

REMARQUE : la protection de documents n'apparaît qu'après activation de l'option **Accéder à la configuration avancée...** (F5) > **Ordinateur** > **Antivirus et antispyware** > **Protection des documents** > **Intégrer dans le système**. La même règle s'applique au contrôle parental : le chemin approprié doit être indiqué dans la configuration avancée.

Une fois que vous avez cliqué sur **Activé**, la boîte de dialogue **Désactiver temporairement la protection** apparaît. Cliquez sur **OK** pour désactiver le composant de sécurité sélectionné. Le menu déroulant **Intervalle** représente la période pendant laquelle le composant sélectionné est désactivé.



Pour réactiver la protection du composant de sécurité désactivé, cliquez sur **Désactivée**.

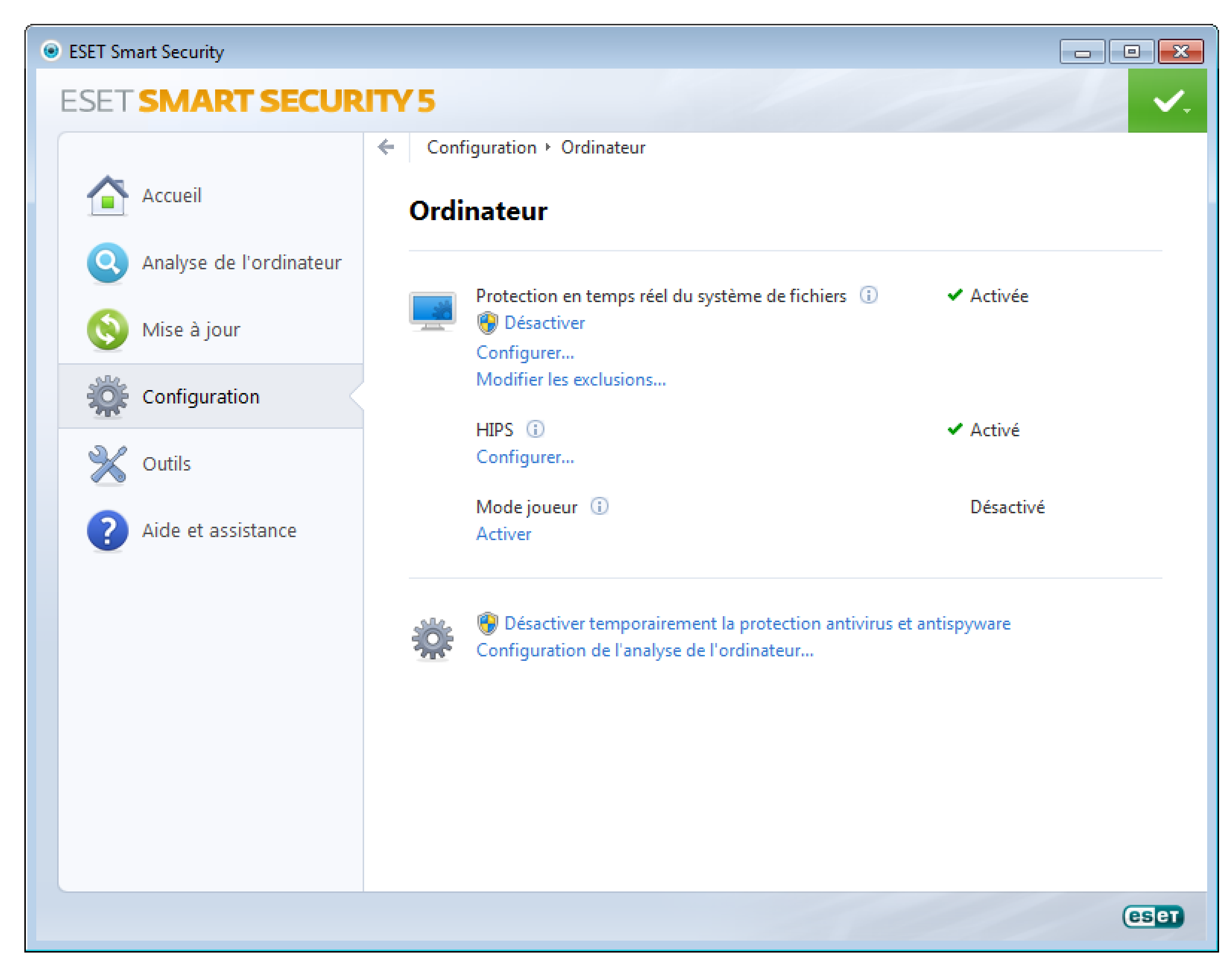
REMARQUE : lorsque vous désactivez la protection à l'aide de cette méthode, tous les composants désactivés de la protection sont activés au redémarrage de l'ordinateur.

D'autres options sont disponibles au bas de la fenêtre de configuration. Utilisez le lien **Activation de produit...** pour ouvrir un formulaire d'enregistrement qui nous permet d'activer le produit de sécurité ESET et de vous envoyer un courrier électronique avec vos données d'authentification (nom d'utilisateur et mot de passe). Pour charger les paramètres de configuration à l'aide d'un fichier de configuration *.xml* ou pour enregistrer les paramètres de configuration dans un fichier de configuration, utilisez l'option **Importer et exporter les paramètres...**

4.1 Ordinateur

Le module **Ordinateur** est accessible dans le volet **Configuration** en cliquant sur l'intitulé **Ordinateur**. Elle affiche un aperçu de tous les modules de protection. Pour désactiver temporairement des modules individuels, cliquez sur **Désactiver** sous le module souhaité. Notez que cela peut abaisser le niveau de protection de l'ordinateur. Pour accéder aux paramètres détaillés de chaque module, cliquez sur **Configurer...**

Cliquez sur **Modifier les exclusions...** pour ouvrir la fenêtre de configuration des exclusions qui permet d'exclure des fichiers et des dossiers de l'analyse.



Désactiver temporairement la protection antivirus et antispyware - Désactive tous les modules de protection antivirus et antispyware. La boîte de dialogue **Désactiver temporairement la protection** avec le menu déroulant **Intervalle de temps** apparaît. Le menu déroulant **Intervalle** représente la période pendant laquelle la protection est désactivée. Cliquez sur **OK** pour confirmer.

Configuration de l'analyse de l'ordinateur... - Cliquez ici pour régler les paramètres d'analyse à la demande (analyse lancée manuellement).

4.1.1 Protection antivirus et antispyware

La protection antivirus et antispyware vous protège des attaques contre le système en contrôlant les échanges de fichiers et de courrier, ainsi que les communications Internet. Si une menace comportant du code malveillant est détectée, le module antivirus peut l'éliminer en la bloquant dans un premier temps, puis en nettoyant, en supprimant ou en mettant en quarantaine l'objet infecté.

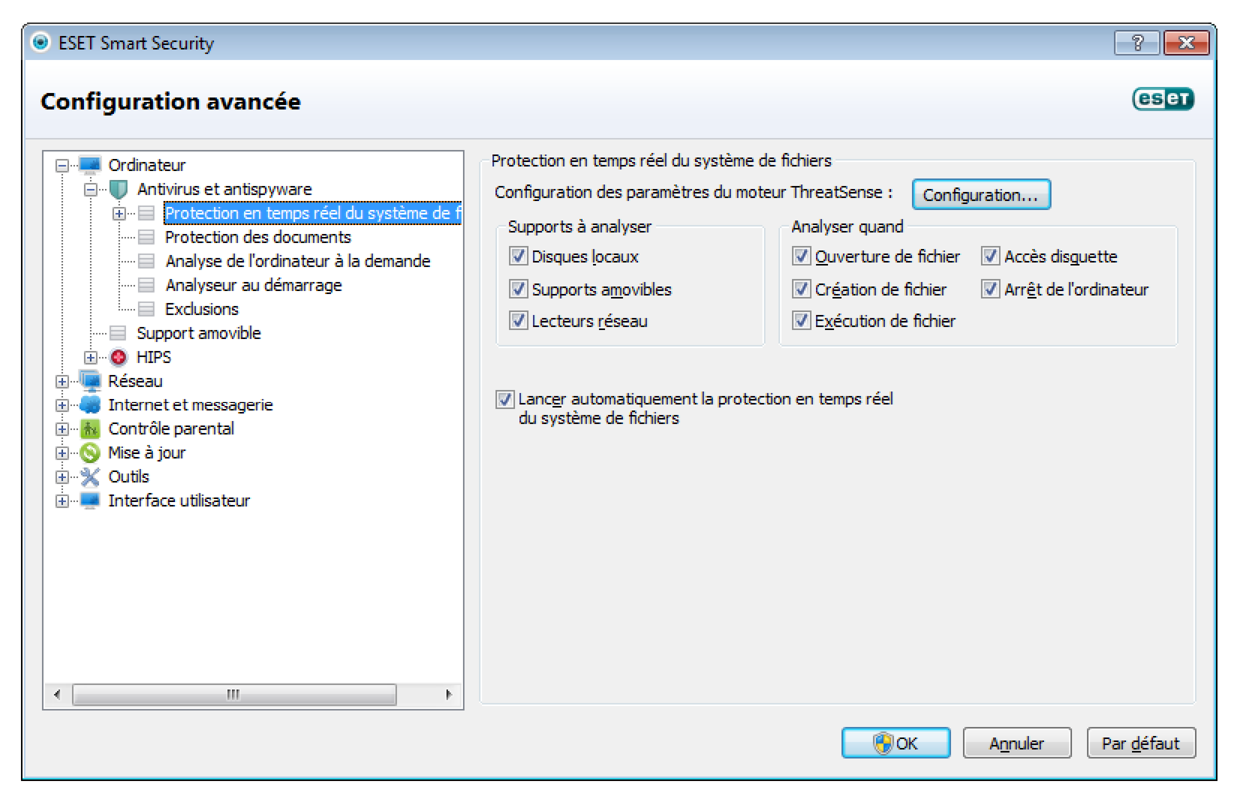
4.1.1.1 Protection en temps réel du système de fichiers

La protection en temps réel du système de fichiers contrôle tous les événements liés à l'antivirus dans le système. Elle analyse tous les fichiers à la recherche de code malveillant lors de l'ouverture, de la création ou de l'exécution de ces fichiers sur l'ordinateur. La protection en temps réel du système de fichiers est lancée au démarrage du système.

La protection en temps réel du système de fichiers vérifie tous les types de supports. Elle est déclenchée par différents événements système, l'accès à un fichier par exemple. Si on utilise les méthodes de détection de la technologie ThreatSense (décrites dans la section Configuration des paramètres du moteur ThreatSense), la protection du système de fichiers en temps réel peut être différente pour les nouveaux fichiers et pour les fichiers existants. Pour les nouveaux fichiers, il est possible d'appliquer un niveau de contrôle plus approfondi.

Pour réduire l'impact de la protection en temps réel sur le système, les fichiers déjà analysés ne sont pas analysés plusieurs fois (sauf s'ils ont été modifiés). Les fichiers sont immédiatement réanalysés après chaque mise à jour de la base des signatures de virus. Ce comportement est configuré à l'aide de l'**optimisation intelligente**. Si cette fonction est désactivée, tous les fichiers sont analysés à chaque accès. Pour modifier cette option, appuyez sur la touche F5 pour ouvrir la fenêtre Configuration avancée et cliquez sur **Ordinateur** > **Antivirus et antispyware** > **Protection des documents** dans la configuration avancée complète. Cliquez ensuite sur le bouton **Configuration...** à côté de l'option **Configuration des paramètres du moteur ThreatSense**, cliquez sur **Autre** et sélectionnez ou désélectionnez l'option **Activer l'optimisation intelligente**.

Par défaut, la protection en temps réel du système de fichiers est lancée au démarrage du système et assure une analyse ininterrompue. Dans certains cas (conflit avec un autre analyseur en temps réel par exemple), il est possible de mettre fin à la protection en temps réel en désactivant l'option **Lancer automatiquement la protection en temps réel du système de fichiers**.



4.1.1.1.1 Supports à analyser

Par défaut, tous les types de supports font l'objet de recherches de menaces potentielles.

Disques locaux - Contrôle tous les disques durs système.

Supports amovibles - Disquettes, CD/DVD, périphériques USB, etc.

Disques réseau - Analyse tous les lecteurs mappés.

Nous recommandons de conserver les paramètres par défaut et de ne les modifier que dans des cas spécifiques, par exemple lorsque l'analyse de certains supports ralentit de manière significative les transferts de données.

4.1.1.1.2 Analyser quand (analyse déclenchée par un événement)

Par défaut, tous les fichiers sont analysés lors de leur ouverture, création ou exécution. Il est recommandé de conserver les paramètres par défaut, car ils offrent le niveau maximal de protection en temps réel pour votre ordinateur.

Ouverture de fichier - Active/désactive l'analyse des fichiers ouverts.

Création de fichier - Active/désactive l'analyse des fichiers créés ou modifiés.

Exécution de fichier - Active/désactive l'analyse des fichiers exécutés.

Accès disquette - Active/désactive l'analyse déclenchée par l'accès au lecteur de disquette.

Arrêt de l'ordinateur - Active ou désactive le contrôle des secteurs d'amorçage du disque dur lors de l'arrêt de l'ordinateur. Bien que les virus d'amorçage soient rares de nos jours, il est recommandé de laisser cette option sélectionnée car le risque d'infection par un virus d'amorçage provenant d'autres sources demeure.

4.1.1.1.3 Options d'analyse avancées

Vous trouverez des options de configuration détaillées dans **Ordinateur** > **Antivirus et antispyware** > **Protection en temps réel du système de fichiers** > **Configuration avancée**.

Autres paramètres ThreatSense pour les fichiers nouveaux et modifiés - La probabilité d'infection des nouveaux fichiers ou des fichiers modifiés est comparativement plus élevée que dans les fichiers existants. C'est la raison pour laquelle le programme vérifie ces fichiers avec des paramètres d'analyse supplémentaires. Outre les méthodes d'analyse basées sur les signatures, le système utilise également l'heuristique avancée, ce qui améliore sensiblement les taux de détection, car l'heuristique peut détecter les nouvelles menaces avant que la mise à jour de la base des signatures de virus n'ait été mise à jour. Outre les nouveaux fichiers, l'analyse porte également sur les fichiers auto-extractibles (.sfx) et les fichiers exécutables compressés (en interne). Par défaut, les archives sont analysées jusqu'au dixième niveau d'imbrication et sont contrôlées indépendamment de leur taille réelle. Désactivez l'option **Paramètres d'analyse d'archive par défaut** pour modifier les paramètres d'analyse d'archive.

Autres paramètres ThreatSense pour les fichiers exécutés : par défaut, l'heuristique avancée n'est pas utilisée lors de l'exécution des fichiers. Toutefois, vous souhaiterez dans certains cas activer cette option (en cochant l'option **Heuristique avancée à l'exécution du fichier**). Notez que l'heuristique avancée peut ralentir l'exécution de certains programmes en raison de l'augmentation de la charge système. Si l'option **Heuristique avancée à l'exécution de fichiers à partir de supports amovibles** est activée et si vous souhaitez exclure certains ports USB du support amovible de l'analyse par heuristique avancée lors de l'exécution des fichiers, cliquez sur **Exceptions...** pour ouvrir la fenêtre d'exclusions du support amovible. Vous pouvez alors personnaliser les paramètres en sélectionnant ou en désélectionnant les cases à cocher qui représentent chaque port.

4.1.1.1.4 Niveaux de nettoyage

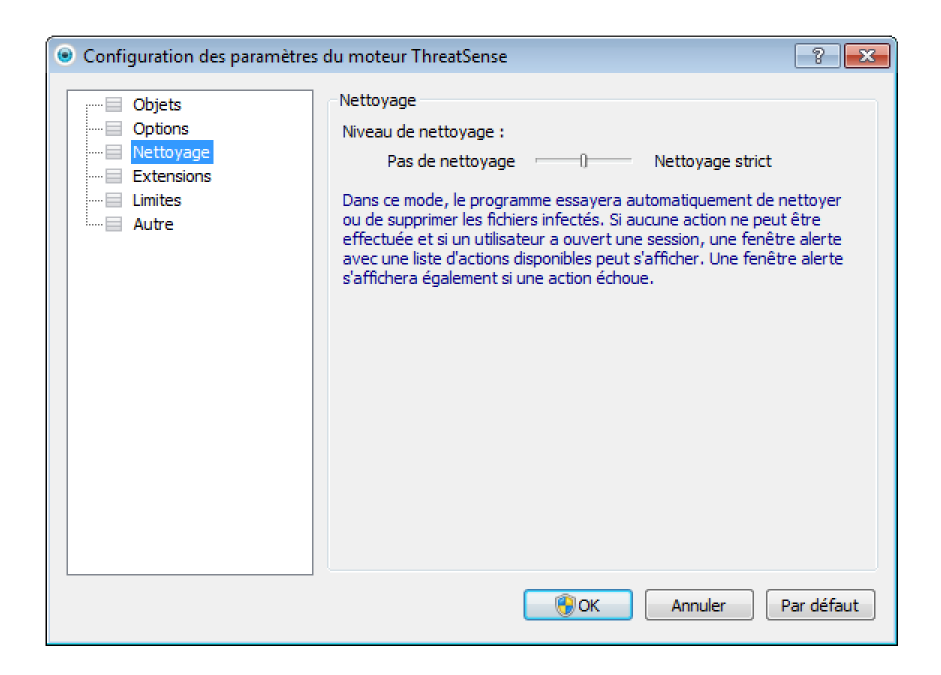
La protection en temps réel comporte trois niveaux de nettoyage (pour y accéder, cliquez sur le bouton **Configuration...** dans la section **Protection en temps réel du système de fichiers**, puis cliquez sur la branche **Nettoyage**).

Pas de nettoyage - Les fichiers infectés ne sont pas nettoyés automatiquement. Le programme affiche alors une fenêtre d'avertissement et laisse l'utilisateur choisir une action. Ce niveau est conçu pour les utilisateurs expérimentés qui connaissent les actions à entreprendre en cas d'infiltration.

Nettoyage standard - Le programme tente de nettoyer ou de supprimer automatiquement tout fichier sur la base d' une action prédéfinie (dépendant du type d'infiltration). La détection et la suppression d'un fichier infecté sont signalées par un message d'information affiché dans l'angle inférieur droit de l'écran. S'il n'est pas possible de sélectionner automatiquement l'action correcte, le programme propose plusieurs actions de suivi. C'est le cas également si une action prédéfinie ne peut pas être menée à bien.

Nettoyage strict - Le programme nettoie ou supprime tous les fichiers infectés. Les seules exceptions sont les fichiers système. S'il n'est pas possible de les nettoyer, l'utilisateur est invité à sélectionner une action dans une fenêtre d'avertissement.

Avertissement : si une archive contient un ou plusieurs fichiers infectés, elle peut être traitée de deux façons différentes. En mode standard (Nettoyage standard), toute l'archive est supprimée si tous ses fichiers sont infectés. En mode de **nettoyage strict**, l'archive est supprimée si elle contient au moins un fichier infecté, quel que soit l'état des autres fichiers qu'elle contient.



4.1.1.1.5 Quand faut-il modifier la configuration de la protection en temps réel

La protection en temps réel est le composant essentiel de la sécurisation du système. Procédez toujours avec prudence lors de la modification des paramètres de ce module. Il est recommandé de ne modifier les paramètres que dans des cas très précis. Ce peut être le cas notamment lorsqu'il y a conflit avec une autre application ou avec l'analyseur en temps réel d'un autre logiciel antivirus.

Après l'installation d'ESET Smart Security, tous les paramètres sont optimisés pour garantir le niveau maximum de système de sécurité aux utilisateurs. Pour restaurer les paramètres par défaut, cliquez sur le bouton **Par défaut** situé dans la partie inférieure droite de la fenêtre **Protection en temps réel** (**Configuration avancée** > **Ordinateur** > **Antivirus et antispyware** > **Protection en temps réel du système de fichiers**).

4.1.1.1.6 Vérification de la protection en temps réel

Pour vérifier que la protection en temps réel fonctionne et détecte les virus, utilisez un fichier de test d'eicar.com. Ce fichier de test est un fichier spécial inoffensif détectable par tous les programmes antivirus. Le fichier a été créé par la société EICAR (European Institute for Computer Antivirus Research) et permet de tester la fonctionnalité des programmes antivirus. Le fichier eicar.com est téléchargeable depuis http://www.eicar.org/download/eicar.com

REMARQUE : avant d'effectuer une vérification de la protection en temps réel, désactivez le pare-feu. S'il est activé, il détecte le fichier et empêche le téléchargement des fichiers de test.

4.1.1.1.7 Que faire si la protection en temps réel ne fonctionne pas ?

Dans ce chapitre, nous décrivons des problèmes qui peuvent survenir lors de l'utilisation de la protection en temps réel et la façon de les résoudre.

La protection en temps réel est désactivée

Si la protection en temps réel a été désactivée par mégarde par un utilisateur, elle doit être réactivée. Pour réactiver la protection en temps réel, sélectionnez **Configuration** dans la fenêtre principale du programme et cliquez sur **Protection en temps réel du système de fichiers**.

Si la protection en temps réel ne se lance pas au démarrage du système, c'est probablement parce que l'option **Lancer automatiquement la protection en temps réel du système de fichiers** est désactivée. Pour activer cette option, sélectionnez Configuration avancée (F5) et cliquez sur **Ordinateur** > **Antivirus et antispyware** > **Protection en temps réel du système de fichiers** dans la configuration avancée complète. Dans la section **Configuration avancée** dans la partie inférieure de la fenêtre, vérifiez que la case **Lancer automatiquement la protection en temps réel du système de fichiers** est cochée.

Si la protection en temps réel ne détecte et ne nettoie pas les infiltrations

Assurez-vous qu'aucun autre programme antivirus n'est installé sur votre ordinateur. Si deux programmes de protection en temps réel sont activés en même temps, il peut y avoir un conflit entre les deux. Nous recommandons de désinstaller tout autre antivirus de votre système.

La protection en temps réel ne démarre pas

Si la protection en temps réel n'est pas lancée au démarrage du système (et si l'option **Lancer automatiquement la protection en temps réel du système de fichiers** est activée), le problème peut provenir de conflits avec d'autres programmes. Dans ce cas, contactez les spécialistes du service client ESET.

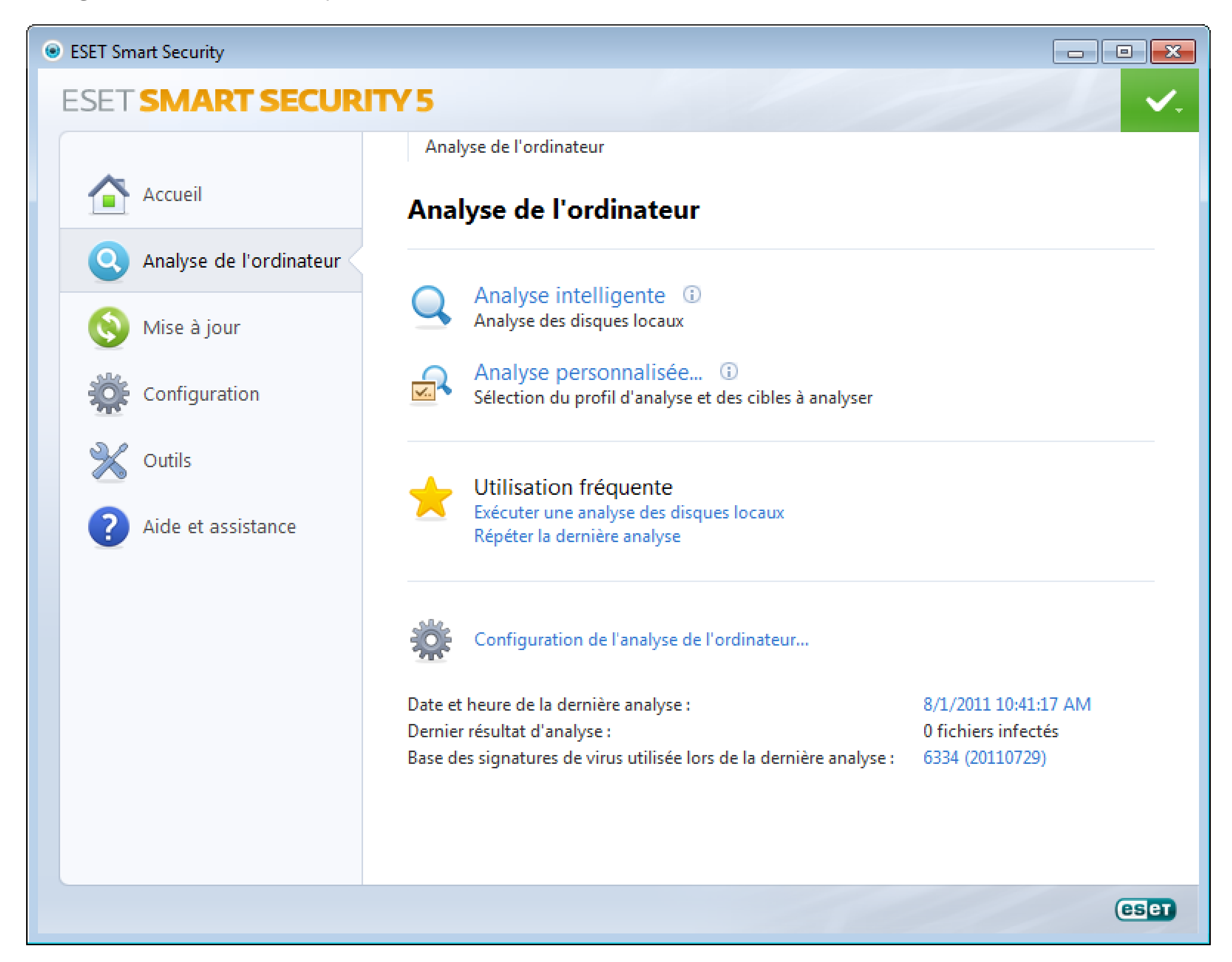
4.1.1.2 Protection des documents

La fonctionnalité de protection des documents analyse les documents Microsoft Office avant leur ouverture, ainsi que les fichiers téléchargés automatiquement par Internet Explorer, tels que des éléments Microsoft ActiveX. **Intégration du système** active le système de protection. Pour modifier cette option, appuyez sur la touche F5 pour ouvrir la fenêtre Configuration avancée et cliquez sur **Ordinateur** > **Antivirus et antispyware** > **Protection des documents** dans la configuration avancée complète. Lorsque cette option est activée, la protection des documents peut être affichée dans la fenêtre principale de ESET Smart Security dans l'option **Configuration** > **Ordinateur**.

Cette fonctionnalité est activée par des applications utilisant Microsoft Antivirus API (par exemple Microsoft Office 2000 et versions ultérieures, ou Microsoft Internet Explorer 5.0 et versions ultérieures).

4.1.1.3 Analyse d'ordinateur

L'analyseur à la demande est une partie importante de votre solution antivirus. Il permet d'analyser des fichiers et des répertoires de votre ordinateur. Pour votre sécurité, il est essentiel que l'ordinateur soit analysé non seulement en cas de suspicion d'une infection, mais aussi régulièrement dans le cadre de mesures de sécurité routinières. Nous vous recommandons d'effectuer des analyses en profondeur de votre système de façon régulière afin de détecter les virus éventuels qui n'auraient pas été bloqués par la protection en temps réel du système de fichiers lors de leur écriture sur le disque. Cela peut se produire si la protection en temps réel du système de fichiers est désactivée au moment de l'infection, si la base des signatures de virus n'est plus à jour ou si le fichier n'a pas été détecté comme virus lors de son enregistrement sur le disque.



Deux types d'**analyses de l'ordinateur** sont disponibles. L'**analyse intelligente** analyse le système sans exiger de reconfiguration des paramètres d'analyse. L'**analyse personnalisée** permet de sélectionner l'un des profils d'analyse prédéfinis, ainsi que de choisir des cibles spécifiques à analyser.

Reportez-vous au chapitre sur la progression de l'analyse pour plus d'informations sur le processus d'analyse.

Nous recommandons d'exécuter une analyse d'ordinateur au moins une fois par mois. L'analyse peut être configurée comme tâche planifiée dans **Outils** > **Planificateur**.

4.1.1.3.1 Type d'analyse

4.1.1.3.1.1 Analyse intelligente

L'analyse intelligente permet de lancer rapidement une analyse de l'ordinateur et de nettoyer les fichiers infectés sans intervention de l'utilisateur. L'analyse intelligente présente l'intérêt d'être facile à utiliser et de ne pas nécessiter de configuration détaillée. L'analyse intelligente vérifie tous les fichiers des disques locaux, et nettoie ou supprime automatiquement les infiltrations détectées. Le niveau de nettoyage est automatiquement réglé sur sa valeur par défaut. Pour plus d'informations sur les types de nettoyage, reportez-vous à la section Nettoyage.

4.1.1.3.1.2 Analyse personnalisée

L'analyse personnalisée est une solution optimale si vous souhaitez spécifier des paramètres d'analyse tels que les cibles et les méthodes d'analyse. L'analyse personnalisée a l'avantage de permettre la configuration précise des paramètres. Les configurations peuvent être enregistrées dans des profils d'analyse définis par l'utilisateur, qui sont utiles pour effectuer régulièrement une analyse avec les mêmes paramètres.

Pour sélectionner des cibles à analyser, sélectionnez **Analyse de l'ordinateur** > **Analyse personnalisée**, puis sélectionnez une option dans le menu déroulant **Cibles à analyser** ou sélectionnez des cibles spécifiques dans l'arborescence. Une cible d'analyse peut également être spécifiée en indiquant le chemin d'accès au dossier ou aux fichiers à inclure. Si vous souhaitez uniquement effectuer une analyse du système sans ajouter d'actions de nettoyage supplémentaires, sélectionnez l'option **Analyse sans nettoyage**. Vous pouvez aussi choisir parmi trois niveaux de nettoyage en cliquant sur **Configuration...** > **Nettoyage**.

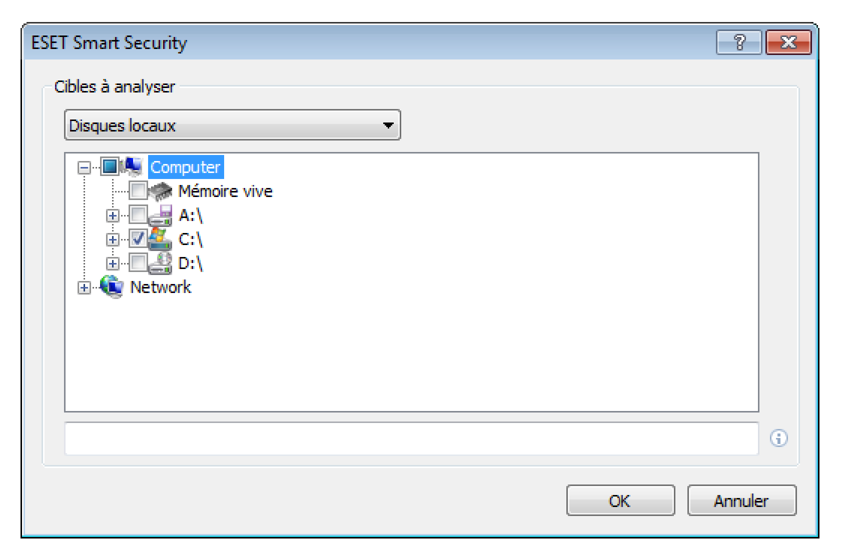
L'exécution d'analyses personnalisées de l'ordinateur convient aux utilisateurs chevronnés qui maîtrisent l'utilisation de programmes antivirus.

4.1.1.3.2 Cibles à analyser

La fenêtre Cibles à analyser permet de définir les objets (mémoire, lecteurs, secteurs, fichiers et dossiers) dans lesquels rechercher des infiltrations. Le menu déroulant **Cibles à analyser** permet de sélectionner des cibles à analyser prédéfinies :

- **Par les paramètres de profil** - Permet de sélectionner les cibles indiquées dans le profil d'analyse sélectionné.
- **Supports amovibles** - Permet de sélectionner les disquettes, les périphériques USB, les CD/DVD, etc.
- **Disques locaux** - Permet de sélectionner tous les disques durs du système.
- **Disques réseau** - Analyse tous les lecteurs réseau mappés.
- **Aucune sélection** - Annule toutes les sélections.

Vous pouvez également définir une cible d'analyse en entrant le chemin du dossier ou des fichiers à inclure dans l'analyse. Sélectionnez les cibles dans l'arborescence des périphériques disponibles sur l'ordinateur.



Pour accéder rapidement à une cible d'analyse ou ajouter directement une cible souhaitée, entrez-la dans le champ vide sous la liste de dossiers. Aucune cible ne doit être sélectionnée dans la structure arborescente et le menu **Cibles à analyser** doit être défini sur **Aucune sélection**.

4.1.1.3.3 Profils d'analyse

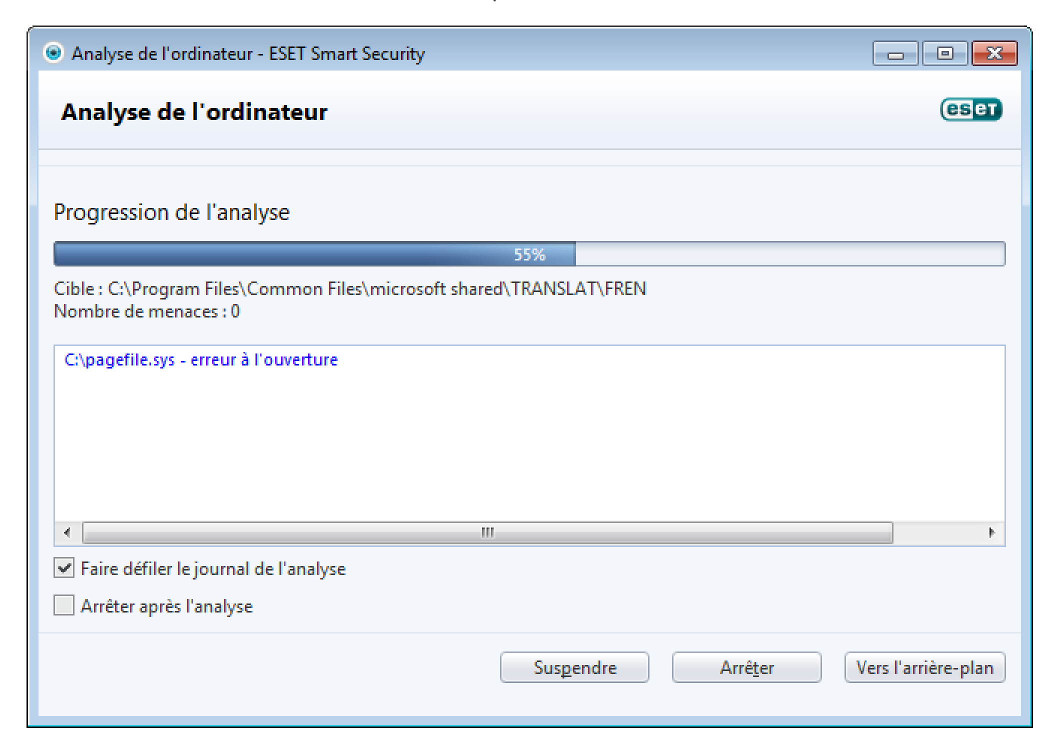
Vos paramètres d'analyse préférés peuvent être enregistrés pour les prochaines analyses. Il est recommandé de créer autant de profils (avec différentes cibles et méthodes, et d'autres paramètres d'analyse) que d'analyses utilisées régulièrement.

Pour créer un nouveau profil, ouvrez la fenêtre Configuration avancée (F5) et cliquez sur **Ordinateur** > **Antivirus et antispyware** > **Analyse de l'ordinateur** > **Profils...**. La fenêtre **Profils de configuration** dispose du menu déroulant **Profil sélectionné** contenant les profils d'analyse existants, ainsi qu'une option permettant de créer un profil. Pour plus d'informations sur la création d'un profil d'analyse correspondant à vos besoins, reportez-vous à la section ThreatSenseConfiguration du moteur ; vous y trouverez une description de chaque paramètre de configuration de l'analyse.

Exemple : Supposons la situation suivante : vous souhaitez créer votre propre profil d'analyse et la configuration d'analyse intelligente est partiellement adéquate. En revanche, vous ne souhaitez analyser ni les fichiers exécutables compressés par un compresseur d'exécutables, ni les applications potentiellement dangereuses. Vous souhaitez effectuer un **nettoyage strict**. Dans la fenêtre **Profils de configuration**, cliquez sur le bouton **Ajouter...**. Saisissez le nom de votre nouveau profil dans le champ **Nom du profil** et sélectionnez **Analyse intelligente** dans le menu déroulant **Copier les paramètres depuis le profil**. Adaptez ensuite les autres paramètres à vos besoins.

4.1.1.3.4 Progression de l'analyse

La fenêtre de progression de l'analyse indique l'état actuel de l'analyse, ainsi que des informations sur le nombre de fichiers contenant du code malveillant qui sont détectés.



REMARQUE : il est normal que certains fichiers, protégés par mot de passe ou exclusivement utilisés par le système (en général *pagefile.sys* et certains fichiers journaux), ne puissent pas être analysés.

Progression de l'analyse - La barre de progression indique le pourcentage des objets déjà numérisés par rapport aux objets qui ne sont pas encore analysés. La valeur est dérivée du nombre total d'objets intégrés dans l'analyse.

Cible - Taille de l'élément analysé et emplacement.

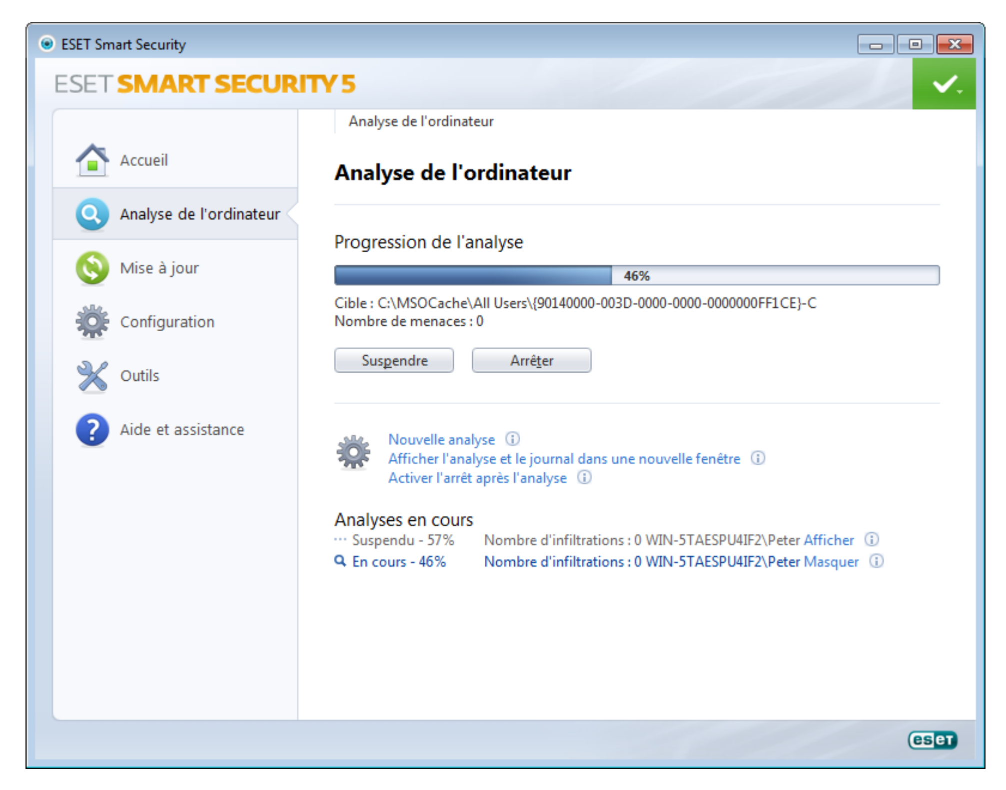
Nombre de menaces - Indique le nombre total de menaces détectées pendant une analyse.

Interrompre - Interrompt une analyse.

Reprendre - Cette option est visible lorsque l'analyse est interrompue. Cliquez sur **Reprendre** pour poursuivre l'analyse.

Arrêter - Met fin à l'analyse.

Vers l'arrière-plan - Vous pouvez exécuter une autre analyse en parallèle. L'analyse en cours s'exécute en arrière-plan.



Cliquez sur **Afficher** pour amener une analyse au premier plan et retourner au processus d'analyse.

Faire défiler le journal de l'analyse - Si cette option est activée, le journal de l'analyse défile automatiquement au fur et à mesure de l'ajout des entrées les plus récentes.

Activer l'arrêt après l'analyse - Active un arrêt planifié à la fin de l'analyse à la demande de l'ordinateur. Une boîte de dialogue de confirmation d'arrêt s'ouvre pendant 60 secondes. Cliquez sur **Annuler** si vous souhaitez désactiver l'arrêt demandé.

4.1.1.4 Analyse au démarrage

La vérification automatique des fichiers au démarrage est effectuée au démarrage du système ou lors de la mise à jour de la base des signatures de virus. Cette analyse dépend de la configuration et des tâches du Planificateur.

Les options d'analyse au démarrage font partie d'une tâche planifiée **Contrôle des fichiers de démarrage du système**. Pour modifier ses paramètres, accédez à **Outils** > **Planificateur**, cliquez sur **Vérification des fichiers de démarrage**, puis sur le bouton **Modifier...**. À la dernière étape, la fenêtre Vérification des fichiers de démarrage s'affichera (reportez-vous à la section suivante pour plus de détails).

Pour des instructions détaillées sur la création et à la gestion de tâches planifiées, voir Création de nouvelles tâches.

4.1.1.4.1 Vérification automatique des fichiers de démarrage

Le menu déroulant **Niveau d'analyse** indique le niveau d'analyse appliqué aux fichiers exécutés au démarrage du système. Les fichiers sont organisés par ordre croissant suivant le nombre de fichiers à analyser :

- **Seulement les fichiers utilisés fréquemment** (nombre minimum de fichiers analysés)
- **Fichiers fréquemment utilisés**
- **Fichiers couramment utilisés**
- **Fichiers rarement utilisés**
- **Tous les fichiers enregistrés** (la plupart des fichiers sont analysés)

Il existe en outre deux groupes de **Niveau d'analyse** :

- **Fichiers exécutés avant la connexion de l'utilisateur** - Contient des fichiers situés à des emplacements leur permettant d'être exécutés sans qu'une session n'ait été ouverte par l'utilisateur (englobe pratiquement tous les emplacements de démarrage tels que services, objets Application d'assistance du navigateur, notification winlogon, entrées de planificateur Windows, DLL connues, etc.).
- **Fichiers exécutés après la connexion de l'utilisateur** - Contient des fichiers situés à des emplacements leur permettant d'être exécutés uniquement après l'ouverture d'une session par l'utilisateur (englobe des fichiers qui ne

sont exécutés que pour un utilisateur spécifique, généralement les fichiers de *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run)*

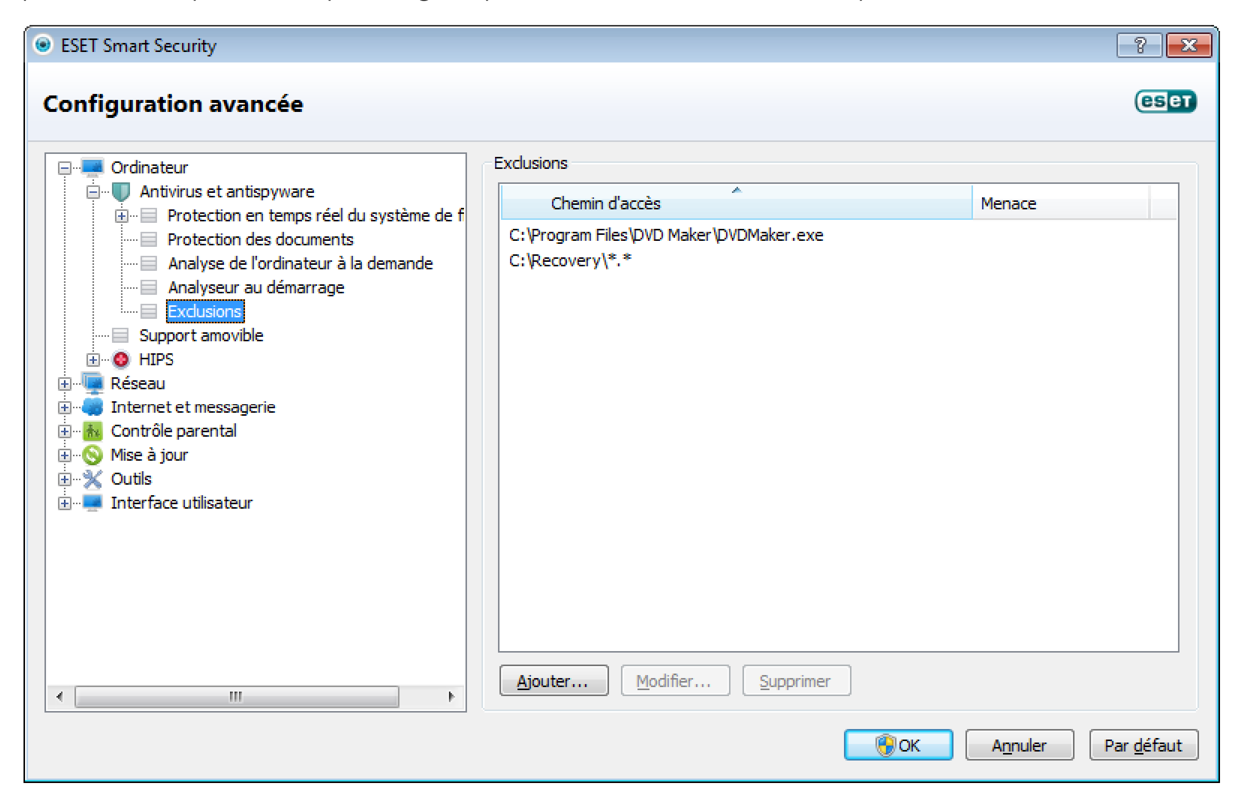
Les listes des fichiers à analyser sont fixes pour chaque groupe.

Priorité d'analyse - Niveau de priorité à appliquer pour lancer l'analyse :

- **Normale** - lorsque le système est moyennement chargé,
- **Faible** - lorsque le système est faiblement chargé,
- **La plus faible** - lorsque la charge du système est la plus faible possible,
- **En période d'inactivité** - la tâche n'est accomplie que lorsque le système est inactif.

4.1.1.5 Exclusions par chemin

Les exclusions permettent d'exclure des fichiers et dossiers de l'analyse. Pour que tous les objets fassent l'objet d'une recherche de menaces, il est recommandé de ne pas modifier ces options. Toutefois, dans certains cas, il peut être utile d'exclure un objet. Par exemple, lorsque les entrées de bases de données volumineuses risquent de ralentir l'ordinateur pendant l'analyse ou lorsque le logiciel présente des conflits avec l'analyse.



Chemin - Chemin d'accès aux fichiers et dossiers exclus.

Menace - Si le nom d'une menace figure à côté d'un fichier exclu, cela signifie que ce fichier n'est exclu que pour cette menace, mais qu'il n'est pas exclu complètement. Par conséquent, si le fichier est infecté ultérieurement par un autre logiciel malveillant, il est détecté par le module antivirus. Ce type d'exclusion ne peut être utilisé que pour certains types d'infiltrations. Il peut être créé soit dans la fenêtre des alertes de menaces qui signale l'infiltration (cliquez sur **Afficher les options avancées** et sélectionnez **Exclure de la détection**), soit dans **Configuration** > **Quarantaine** à l'aide de l'option du menu contextuel **Restaurer et exclure de la détection** du fichier en quarantaine.

Ajouter... - Exclut les objets de la détection.

Modifier... - Permet de modifier des entrées sélectionnées.

Supprimer - Supprime les entrées sélectionnées.

Pour exclure un objet de l'analyse :

1. Cliquez sur **Ajouter...**,
2. Entrez le chemin d'un objet ou sélectionnez-le dans l'arborescence.

Vous pouvez utiliser des caractères génériques pour indiquer un groupe de fichiers. Un point d'interrogation (?) représente un seul caractère variable tandis qu'un astérisque (*) représente une chaîne variable de zéro caractère ou plus.

Exemples

- Si vous souhaitez exclure tous les fichiers d'un dossier, tapez le chemin d'accès au dossier et utilisez le masque « *.* ».
- Pour exclure un disque complet avec tous ses fichiers et sous-dossiers, utilisez le masque « D:\ »
- Si vous ne souhaitez exclure que les fichiers doc, utilisez le masque « *.doc ».
- Si le nom d'un fichier exécutable comporte un certain nombre de caractères variables dont vous ne connaissez que le premier (par exemple « D »), utilisez le format suivant : « D????.exe ». Les points d'interrogation remplacent les caractères manquants (inconnus).

4.1.1.6 Configuration des paramètres du moteur ThreatSense

ThreatSense est une technologie qui comprend de nombreuses méthodes de détection de menaces complexes. C'est une technologie proactive : elle fournit une protection dès les premières heures de propagation d'une nouvelle menace. Elle utilise une combinaison de plusieurs méthodes (analyse de code, émulation de code, signatures génériques, signatures de virus) qui se conjuguent pour améliorer sensiblement la sécurité du système. Ce moteur d'analyse est capable de contrôler plusieurs flux de données simultanément, ce qui maximise l'efficacité et le taux de détection. La technologie ThreatSense élimine avec succès les rootkits.

Les options de configuration de la technologie ThreatSense permettent de spécifier plusieurs paramètres d'analyse :

- les types de fichiers et les extensions à analyser ;
- la combinaison de plusieurs méthodes de détection ;
- les niveaux de nettoyage, etc.

Pour ouvrir la fenêtre de configuration, cliquez sur le bouton **Configuration...** situé dans la fenêtre de configuration de tous les modules qui utilisent la technologie ThreatSense (reportez-vous aux informations ci-dessous). Chaque scénario de sécurité peut exiger une configuration différente. ThreatSense est configurable individuellement pour les modules de protection suivants :

- protection en temps réel du système de fichiers ;
- protection des documents ;
- protection du client de messagerie ;
- Protection de l'accès au Web et antihameçonnage,
- analyse de l'ordinateur.

Les paramètres ThreatSense sont spécifiquement optimisés pour chaque module et leur modification peut avoir une incidence significative sur le fonctionnement du système. Par exemple, en modifiant les paramètres pour toujours analyser les Fichiers exécutables compressés par un compresseur d’exécutables ou pour autoriser l'heuristique avancée dans la protection en temps réel du système de fichiers, vous pouvez dégrader les performances du système (normalement, seuls les fichiers nouvellement créés sont analysés par ces méthodes). Il est donc recommandé de ne pas modifier les paramètres par défaut de ThreatSense pour tous les modules, à l'exception du module Analyse de l'ordinateur.

4.1.1.6.1 Objets

La section **Objets** permet de définir les fichiers et les composants de l'ordinateur qui vont faire l'objet d'une analyse visant à rechercher les éventuelles infiltrations.

Mémoire vive - Lance une analyse visant à rechercher les menaces qui attaquent la mémoire vive du système.

Secteurs d'amorçage - Analyse les secteurs d'amorçage afin de détecter la présence éventuelle de virus dans l'enregistrement d'amorçage principal.

Fichiers des courriers électroniques - Le programme prend en charge les extensions suivantes : DBX (Outlook Express) et EML.

Archives - Le programme prend en charge les extensions suivantes : ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE et de nombreuses autres extensions.

Archives auto-extractibles - Les archives auto-extractibles (SFX) n'ont pas besoin de programmes spécialisés pour être décompressées.

Fichiers exécutables compressés par un compresseur d'exécutables - Contrairement aux archiveurs standard, ces fichiers se décompressent en mémoire. Outre les compacteurs statiques standard (UPX, yoda, ASPack, FSG, etc.), l'analyseur prend en charge de nombreux autres types de compacteurs (grâce à l'émulation de code).

4.1.1.6.2 Options

Utilisez la section **Options** pour sélectionner les méthodes à utiliser lors de la recherche d'infiltrations dans le système. Les options disponibles sont les suivantes :

Heuristique - La méthode heuristique utilise un algorithme d'analyse de l'activité (malveillante) des programmes. Elle présente l'avantage d'identifier un code malveillant qui n'existait pas ou qui n'était pas connu par la base de signatures de virus antérieure. Cette méthode présente néanmoins l'inconvénient d'une probabilité (très faible) de fausses alarmes.

Heuristique avancée/ADN/Signatures intelligentes - La méthode heuristique avancée utilise un algorithme heuristique développé par ESET, optimisé pour la détection des vers d'ordinateur et des chevaux de Troie, et écrit dans un langage de programmation de haut niveau. Grâce à l'heuristique avancée, les capacités de détection du programme sont très élevées. Les signatures peuvent détecter et identifier les virus avec grande efficacité. Grâce au système de mise à jour automatique, les nouvelles signatures peuvent être disponibles dans les quelques heures qui suivent la détection des menaces. L'inconvénient des signatures est qu'elles ne détectent que les virus qu'elles connaissent (ou leurs versions légèrement modifiées).

Les **applications potentiellement indésirables** ne sont pas nécessairement malveillantes, mais elles sont susceptibles d'affecter les performances de votre ordinateur. Ces applications sont habituellement installées après consentement. Si elles sont présentes sur votre ordinateur, votre système se comporte différemment (par rapport à son état avant l'installation). Voici les changements les plus significatifs :

- affichage de nouvelles fenêtres (fenêtres contextuelles, publicités) ;
- activation et exécution de processus cachés ;
- augmentation de l'utilisation des ressources système ;
- modification des résultats de recherche ;
- communication de l'application avec des serveurs distants.

Applications potentiellement dangereuses - Applications potentiellement dangereuses correspond à la classification utilisée pour les logiciels commerciaux légitimes. Cette catégorie comprend les programmes d'accès à distance, les applications de décodage des mots de passe ou les keyloggers (programmes qui enregistrent chaque frappe au clavier de l'utilisateur). Cette option est désactivée par défaut.

ESET Live Grid - Grâce à la technologie de réputation d'ESET, les informations sur les fichiers analysés sont comparées aux données issues du système ESET Live Grid basé sur le cloud computing. Cette comparaison permet d'améliorer la détection tout en accélérant l'analyse.

4.1.1.6.3 Nettoyage

Les paramètres de nettoyage déterminent le comportement de l'analyseur lors du nettoyage des fichiers infectés. Trois niveaux de nettoyage sont possibles :

Pas de nettoyage - Les fichiers infectés ne sont pas nettoyés automatiquement. Le programme affiche alors une fenêtre d'avertissement et laisse l'utilisateur choisir une action. Ce niveau est conçu pour les utilisateurs expérimentés qui connaissent les actions à entreprendre en cas d'infiltration.

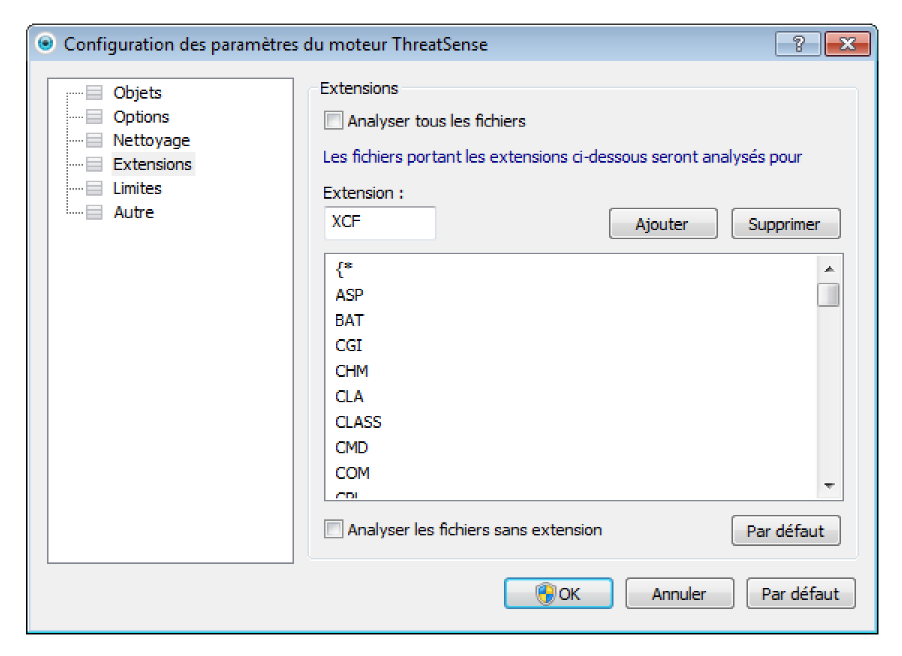
Nettoyage standard - Le programme tente de nettoyer ou de supprimer automatiquement tout fichier sur la base d' une action prédéfinie (dépendant du type d'infiltration). La détection et la suppression d'un fichier infecté sont signalées par un message d'information affiché dans l'angle inférieur droit de l'écran. S'il n'est pas possible de sélectionner automatiquement l'action correcte, le programme propose plusieurs actions de suivi. C'est le cas également si une action prédéfinie ne peut pas être menée à bien.

Nettoyage strict - Le programme nettoie ou supprime tous les fichiers infectés. Les seules exceptions sont les fichiers système. S'il n'est pas possible de les nettoyer, l'utilisateur est invité à sélectionner une action dans une fenêtre d'avertissement.

Avertissement : si une archive contient un ou plusieurs fichiers infectés, elle peut être traitée de deux façons différentes. En mode standard (Nettoyage standard), toute l'archive est supprimée si tous ses fichiers sont infectés. En mode de **nettoyage strict**, l'archive est supprimée si elle contient au moins un fichier infecté, quel que soit l'état des autres fichiers qu'elle contient.

4.1.1.6.4 Extension

L'extension est la partie du nom de fichier située après le point. Elle définit le type et le contenu du fichier. Cette section de la configuration des paramètres ThreatSense vous permet de définir les types de fichiers à analyser.



Par défaut, tous les fichiers sont analysés, quelle que soit leur extension. Toutes les extensions peuvent être ajoutées à la liste des fichiers exclus de l'analyse. Si l'option **Analyser tous les fichiers** est désélectionnée, la liste change et affiche toutes les extensions des fichiers analysés.

Pour activer l'analyse des fichiers sans extension, sélectionnez l'option **Analyser les fichiers sans extension**. L'option **Ne pas analyser les fichiers sans extension** devient disponible lorsque l'option **Analyser tous les fichiers** est activée.

L'exclusion de fichiers peut être utile si l'analyse de certains types de fichiers provoque un dysfonctionnement du programme utilisant ces extensions. Par exemple, il peut être judicieux d'exclure les extensions .edb, .eml et .tmp si vous utilisez le serveur Microsoft Exchange.

Les boutons **Ajouter** et **Supprimer** permettent d'activer ou d'empêcher l'analyse des fichiers portant certaines extensions. Le fait de taper une **extension** active le bouton **Ajouter** et permet d'ajouter cette nouvelle extension à la liste. Sélectionnez une extension dans la liste, puis cliquez sur **Supprimer** pour supprimer l'extension de la liste.

Vous pouvez utiliser les symboles spéciaux « * » (astérisque) et « ? » (point d'interrogation). L'astérisque remplace n'importe quelle chaîne de caractères, tandis que le point d'interrogation remplace n'importe quel caractère. Un soin particulier doit être apporté à la spécification des adresses exclues, car la liste ne doit contenir que des adresses sûres et de confiance. De la même manière, veillez à employer correctement les symboles « * » et « ? » dans cette liste.

Pour n'analyser que l'ensemble des extensions par défaut, cliquez sur le bouton **Défaut**, puis sur **Oui** pour confirmer.

4.1.1.6.5 Limites

La section Limites permet de spécifier la taille maximale des objets et les niveaux d'imbrication des archives à analyser :

Taille maximale d'objet - Définit la taille maximale des objets à analyser. Le module antivirus n'analyse que les objets d'une taille inférieure à celle spécifiée. Cette option ne doit être modifiée que par des utilisateurs expérimentés et qui ont des raisons particulières d'exclure de l'analyse des objets de plus grande taille. Valeur par défaut : *illimité*.

Durée d'analyse maximale pour l'objet (s) - Définit la durée maximum attribuée à l'analyse d'un objet. Si la valeur de ce champ a été définie par l'utilisateur, le module antivirus cesse d'analyser un objet une fois ce temps écoulé, que l'analyse soit terminée ou non. Valeur par défaut : *illimité*.

Niveau d'imbrication des archives - Spécifie la profondeur maximale d'analyse des archives. Valeur par défaut : *10*.

Taille maximale de fichier dans l'archive - Cette option permet de spécifier la taille maximale des fichiers (après extraction) à analyser contenus dans les archives. Valeur par défaut : *illimité*.

Si l'analyse d'une archive prend fin prématurément pour ces raisons, la case de l'archive reste non vérifiée.

Remarque : il n'est pas recommandé de modifier les valeurs par défaut. Dans des circonstances normales, il n'y a aucune raison de le faire.

4.1.1.6.6 Autre

Vous pouvez configurer les options suivantes dans la section **Autre** :

Journaliser tous les objets - Si cette option est sélectionnée, le fichier journal affiche tous les fichiers analysés, même ceux qui ne sont pas infectés. Par exemple, si une infiltration est détectée dans une archive, le journal répertorie également les fichiers nettoyés contenus dans l'archive.

Activer l'optimisation intelligente - Lorsque cette option est sélectionnée, les paramètres optimaux sont utilisés de manière à garantir le niveau d'analyse le plus efficace tout en conservant la meilleure vitesse d'analyse. Les différents modules de protection proposent une analyse intelligente en utilisant différentes méthodes et en les appliquant à des types de fichiers spécifiques. Si l'option Activer l'optimisation intelligente est désactivée, seuls les paramètres définis par l'utilisateur dans le noyau ThreatSense des différents modules sont appliqués lors de la réalisation d'une analyse.

Lorsque vous configurez les paramètres du moteur ThreatSense pour l'analyse d'un ordinateur, vous disposez également des options suivantes :

Analyser les flux de données alternatifs (ADS) - Les flux de données alternatifs (ADS) utilisés par le système de fichiers NTFS sont des associations de fichiers et de dossiers que les techniques d'analyse ordinaires ne permettent pas de détecter. De nombreuses infiltrations tentent d'éviter la détection en se faisant passer pour des flux de données alternatifs.

Exécuter les analyses en arrière-plan avec une priorité faible - Toute séquence d'analyse consomme une certaine quantité de ressources système. Si vous utilisez des programmes qui exigent une grande quantité de ressources système, vous pouvez activer l'analyse en arrière-plan à faible priorité de manière à réserver des ressources pour vos applications.

Conserver la date et l'heure du dernier accès - Sélectionnez cette option pour conserver l'heure d'accès d'origine des fichiers analysés au lieu de les mettre à jour (par exemple pour les utiliser avec des systèmes de sauvegarde de données).

Faire défiler le journal de l'analyse - Cette option permet d'autoriser/interdire le défilement du journal. Si cette option est sélectionnée, les informations défilent vers le haut dans la fenêtre d'affichage.

4.1.1.7 Une infiltration est détectée

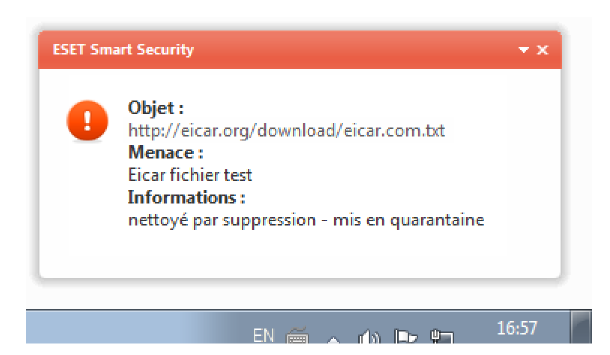
Des infiltrations peuvent atteindre le système à partir de différents points d'entrée : pages Web, dossiers partagés, courrier électronique ou périphériques amovibles (USB, disques externes, CD, DVD, disquettes, etc.).

Comportement standard

Pour illustrer de manière générale la gestion des infiltrations par ESET Smart Security, celles-ci peuvent être détectées par les fonctions

- protection en temps réel du système de fichiers ;
- protection de l'accès au Web et antihameçonnage ;,
- protection du client de messagerie, ou
- analyse de l'ordinateur à la demande.

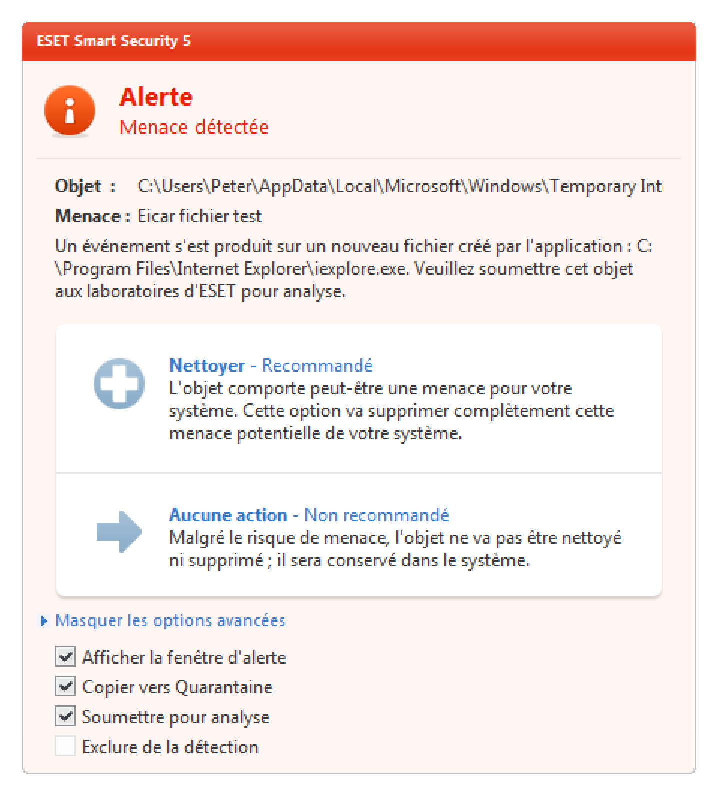
Chaque fonction utilise le niveau de nettoyage standard et tente de nettoyer le fichier et de le déplacer en Quarantaine ou met fin à la connexion. Une fenêtre de notification s'affiche dans la zone de notification, dans l'angle inférieur droit de l'écran. Pour plus d'informations sur les niveaux et le comportement de nettoyage, voir Nettoyage.



Nettoyage et suppression

Si aucune action n'est prédéfinie pour le module de protection du système de fichiers en temps réel, vous êtes invité à sélectionner une option dans une fenêtre d'avertissement. Généralement, les options **Nettoyer**, **Supprimer** et **Aucune action** sont disponibles. Il est n'est pas recommandé de sélectionner **Aucune action**, car cette option laissera les fichiers infectés non nettoyés. La seule exception concerne les situations où vous êtes sûr qu'un fichier est inoffensif et qu'il a été détecté par erreur.

Utilisez le nettoyage si un fichier sain a été attaqué par un virus qui y a joint du code malveillant. Dans ce cas, essayez d'abord de nettoyer le fichier infecté pour le restaurer dans son état d'origine. Si le fichier se compose uniquement de code malveillant, il est supprimé.



Si un fichier infecté est « verrouillé » ou utilisé par un processus système, il n'est généralement supprimé qu'après avoir été déverrouillé (normalement, après un redémarrage du système).

Suppression de fichiers dans les archives

En mode de nettoyage par défaut, l'archive complète n'est supprimée que si elle ne contient que des fichiers infectés et aucun fichier sain. Autrement dit, les archives ne sont pas supprimées si elles contiennent également des fichiers sains. Soyez prudent si vous choisissez un nettoyage strict ; dans ce mode, l'archive est supprimée si elle contient au moins un fichier infecté, quel que soit l'état des autres fichiers qu'elle contient.

Si votre ordinateur montre des signes d'infection par un logiciel malveillant (ralentissement, blocages fréquents, etc.), nous recommandons d'effectuer les opérations suivantes :

- Ouvrez ESET Smart Security et cliquez sur Analyse de l'ordinateur.
- Cliquez sur **Analyse intelligente** (pour plus d'informations, voir Analyse intelligente),
- Lorsque l'analyse est terminée, consultez le journal pour connaître le nombre de fichiers analysés, infectés et nettoyés.

Si vous ne souhaitez analyser qu'une certaine partie de votre disque, cliquez sur **Analyse personnalisée** et sélectionnez des cibles à analyser.

4.1.2 Supports amovibles

ESET Smart Security permet de contrôler automatiquement les supports amovibles (CD/DVD/USB...). Ce module permet d'analyser, de bloquer ou d'ajuster les filtres étendus/autorisations, et de sélectionner la façon dont l'utilisateur peut accéder à un périphérique et l'utiliser. Cela peut être utile si l'administrateur souhaite empêcher les utilisateurs d'utiliser des supports amovibles avec du contenu non sollicité.

Supports amovibles pris en charge

- CD/DVD/Blu-ray
- Clé USB
- Lecteur USB
- FireWire

Action à entreprendre après l'insertion de support amovible - Sélectionnez l'action par défaut à exécuter lors de l'insertion d'un support amovible dans l'ordinateur (CD/DVD/USB). Si l'option **Afficher les options d'analyse** est sélectionnée, une notification vous autorise à choisir l'action adéquate :

- **Analyser maintenant** - Le support amovible inséré fait l'objet d'une analyse à la demande.
- **Analyser ultérieurement** - Aucune action n'est exécutée et la fenêtre **Nouveau périphérique détecté** se ferme.
- **Configuration...** - Ouvre la section de configuration des supports amovibles.

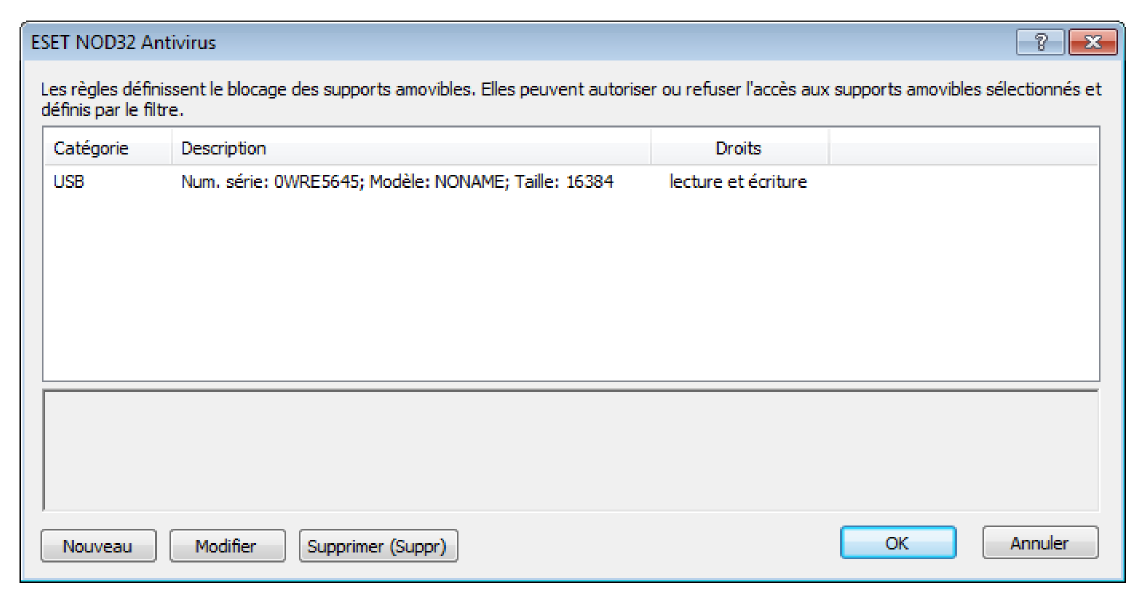


Règles de blocage de support amovible - Sélectionnez cette option pour bloquer tous les supports amovibles connectés à l'ordinateur. Si vous voulez que certains supports soient disponibles, excluez-les du blocage.

Cliquez sur **Règles...** pour autoriser ou bloquer l'accès au support amovible sélectionné. Vous pouvez gérer dans cette fenêtre des règles étendues pour le support amovible. Les règles peuvent être filtrées par exemple par taille de support, numéro de série et type de périphérique. Chaque règle dispose de ses propres autorisations : vous pouvez donc autoriser, limiter ou bloquer l'accès au support amovible sélectionné. Vous trouverez davantage d'informations sur l'analyse et le blocage des supports amovibles au chapitre Filtres permettant de définir l'accès aux périphériques.

4.1.2.1 Filtres permettant de définir l'accès aux périphériques

La fenêtre des filtres permettant de définir l'accès aux périphériques affiche les règles étendues pour le support amovible.



Catégorie - Type de support amovible (CD/DVD/USB).

Description - Description des règles de filtre définissant l'accès aux périphériques.

Droits - Autorisations associées de certains périphériques qui correspondent aux critères définis par le filtre.

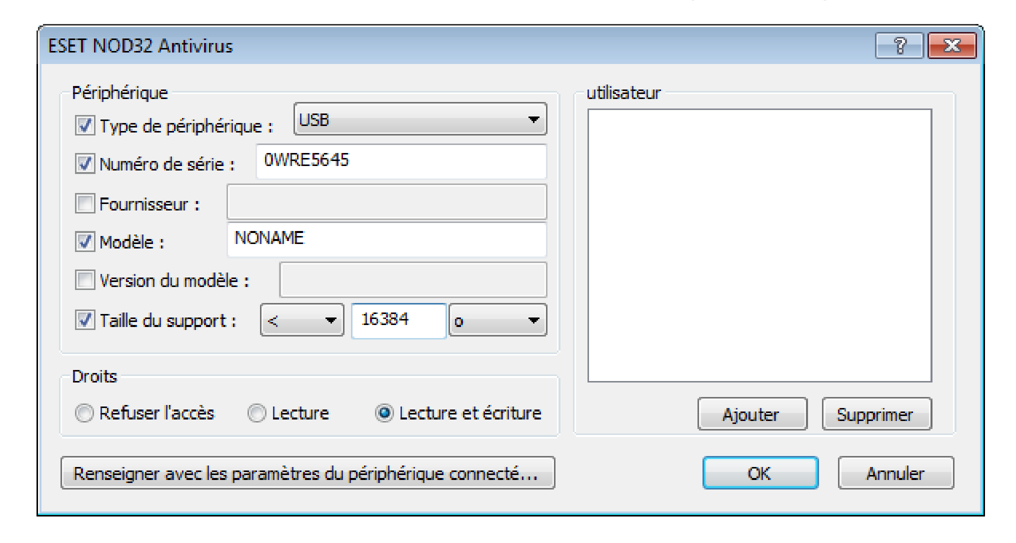
Nouveau - Crée une règle de filtrage des supports amovibles.

Modifier - Sélectionnez une ligne et cliquez sur ce bouton pour modifier la règle existante.

Supprimer (Suppr) - Supprime la règle sélectionnée.

4.1.2.2 Nouveau filtre/Changer de filtre

Cette fenêtre vous permet de créer ou de modifier la règle de filtrage existante.



Périphérique

- **Type de périphérique** - Choisissez le type de support amovible dans la liste (CD/DVD/USB).
- **Numéro de série** - Un support amovible a généralement sont propre numéro de série. S'il s'agit d'un CD/DVD, le numéro de série se trouve sur le support proprement dit, pas sur le lecteur de CD.
- **Éditeur** - Filtrage par nom ou ID de fournisseur.
- **Modèle** - Nom du périphérique.
- **Version du modèle** - La version du périphérique, le cas échéant.
- **Taille du support** - En activant cette option, vous pouvez définir des filtres conditionnels (supérieur à, égal, inférieur à) par taille de support (octets, méga-octets, etc.).

Droits

- **Refuser l'accès** - L'accès au périphérique est refusé.
- **Lecture** - L'utilisateur peut lire les fichiers depuis un support amovible donné.
- **Lecture et écriture** - Contrôle complet sur le support amovible.

Utilisateur

- **Ajouter** - Ouvre la boîte de dialogue **Type d'objet : utilisateurs ou groupes** qui permet de sélectionner les utilisateurs voulus.
- **Supprimer** - Supprime l'utilisateur sélectionné du filtre.

Renseigner avec les paramètres du périphérique connecté... - Cliquez sur cette option pour sélectionner les paramètres du périphérique de support amovible connecté à votre ordinateur.

4.1.3 Système de détection d'intrusion au niveau de l'hôte (HIPS)

Le **système HIPS (Host Intrusion Prevention System)** protège votre système des logiciels malveillants et de toute activité non souhaitée qui pourrait avoir une incidence sur votre ordinateur. Il utilise l'analyse avancée des comportements, associée aux fonctionnalités de détection du filtre réseau qui surveille les processus en cours, les fichiers et les clés de registre. Le système HIPS diffère de la protection en temps réel du système de fichiers et ce n'est pas un pare-feu. Il surveille uniquement les processus en cours d'exécution au sein du système d'exploitation.

Le système HIPS est disponible dans **Configuration avancée** (F5) en cliquant sur **Ordinateur** > **HIPS**. L'état HIPS (activé/désactivé) apparaît dans la fenêtre principale ESET Smart Security, dans le volet **Configuration**, dans la partie droite de la section **Ordinateur**.

Les paramètres HIPS se trouvent dans la **Configuration avancée** (F5). Pour accéder au système HIPS dans l'arborescence de configuration avancée, cliquez sur **Ordinateur** > **HIPS**. L'état HIPS (activé/désactivé) apparaît dans la fenêtre principale de ESET Smart Security, dans le volet **Configuration**, dans la partie droite de la section Ordinateur.

Avertissement : les modifications apportées aux paramètres HIPS ne sont effectuées que par un utilisateur expérimenté.

ESET Smart Security intègre la technologie *Auto-défense* qui empêche les logiciels malveillants d'endommager ou de désactiver la protection antivirus et antispyware ; vous avez la garantie que votre système est protégé en permanence. Les modifications apportées aux paramètres **Activer HIPS** et **Activer l'auto-défense** entrent en vigueur après le redémarrage du système d'exploitation Windows. La désactivation de l'intégralité du système **HIPS** nécessite également un redémarrage de l'ordinateur.

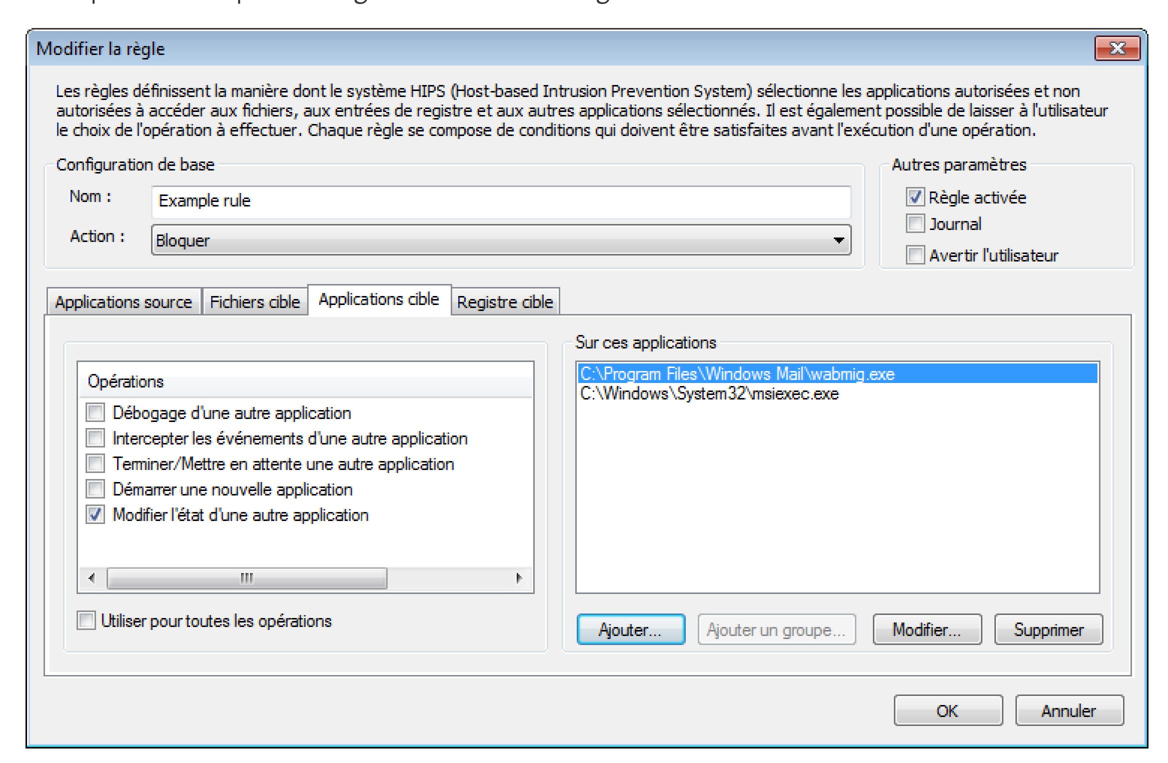
Le filtrage peut être effectué dans l'un des quatre modes :

- **Mode automatique avec règles** - Les opérations sont activées, à l'exception des règles prédéfinies qui protègent votre système.
- **Mode interactif** - L'utilisateur est invité à confirmer les opérations.
- **Mode basé sur des règles personnalisées** - Les opérations sont bloquées.
- **Mode d'apprentissage** - Les opérations sont activées et une règle est créée après chaque opération. Les règles créées dans ce mode peuvent être affichées dans l'**éditeur de règles**, mais leur niveau de priorité est inférieur à celui des règles créées à la main ou en mode automatique. Après la sélection du **mode d'apprentissage**, l'option **Notifier l'expiration de mode d'apprentissage dans X jours** devient active. À la fin de cette période, le mode d'apprentissage est de nouveau désactivé. La durée maximum est de 14 jours. À l'issue de cette période, une fenêtre contextuelle apparaît dans laquelle vous pouvez modifier les règles et sélectionner un autre mode de filtrage.

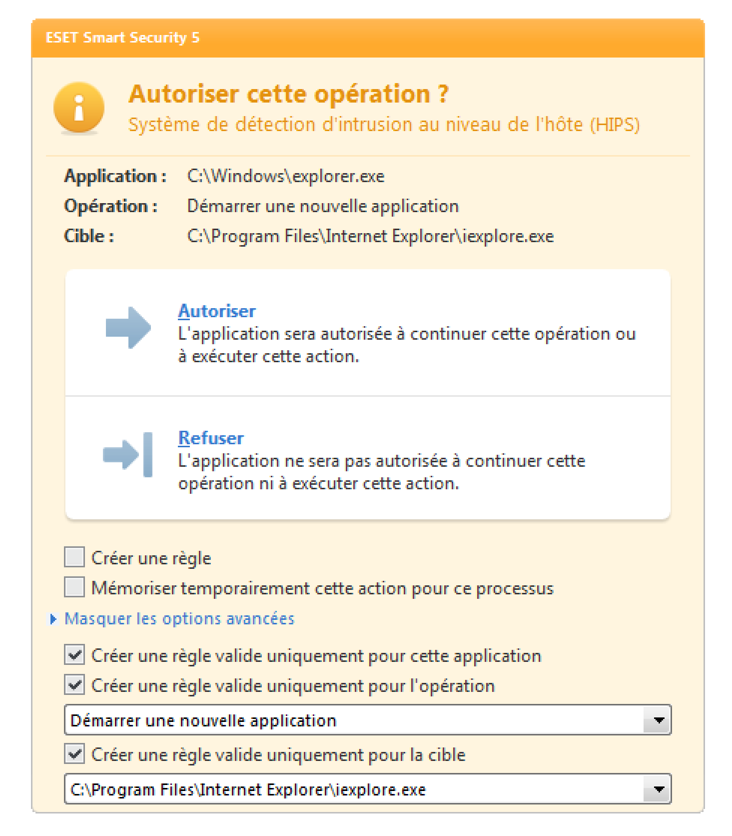
Le système HIPS surveille les événements dans le système d'exploitation et réagit en fonction de règles qui sont semblables à celles utilisées par le pare-feu personnel. Cliquez sur **Configurer les règles...** pour ouvrir la fenêtre de gestion des règles HIPS. Cette fenêtre vous permet de sélectionner, de créer, de modifier ou de supprimer des règles.

Dans l'exemple suivant, nous allons montrer comment limiter le comportement indésirable des applications :

1. Nommez la règle et sélectionnez **Bloquer** dans le menu déroulant **Action**.
2. Ouvrez l'onglet **Applications cibles**. Laissez l'onglet **Applications source** vide pour appliquer la nouvelle règle à toutes les applications qui tentent d'effectuer l'une des opérations cochées dans la liste **Opérations** sur des applications répertoriées dans la liste **Sur ces applications**.
3. Sélectionnez **Modifier l'état d'une autre application** (toutes les opérations sont décrites dans l'aide du produit, appuyez sur la touche F1 dans la fenêtre qui est identique à l'image ci-dessous).
4. Ajoutez une ou plusieurs applications que vous souhaitez protéger.
5. Activez l'option **Avertir l'utilisateur** pour afficher une notification chaque fois que la règle est appliquée.
6. Cliquez sur **OK** pour enregistrer la nouvelle règle.



Une boîte de dialogue apparaît chaque fois que l'option par défaut est **Demander**. L'utilisateur peut choisir de **refuser** ou d'**autoriser** l'opération. Si l'utilisateur ne choisit aucune action dans la période donnée, une nouvelle action est sélectionnée en fonction des règles.



La boîte de dialogue permet de créer une règle en fonction de toute nouvelle action détectée par le système HIPS puis

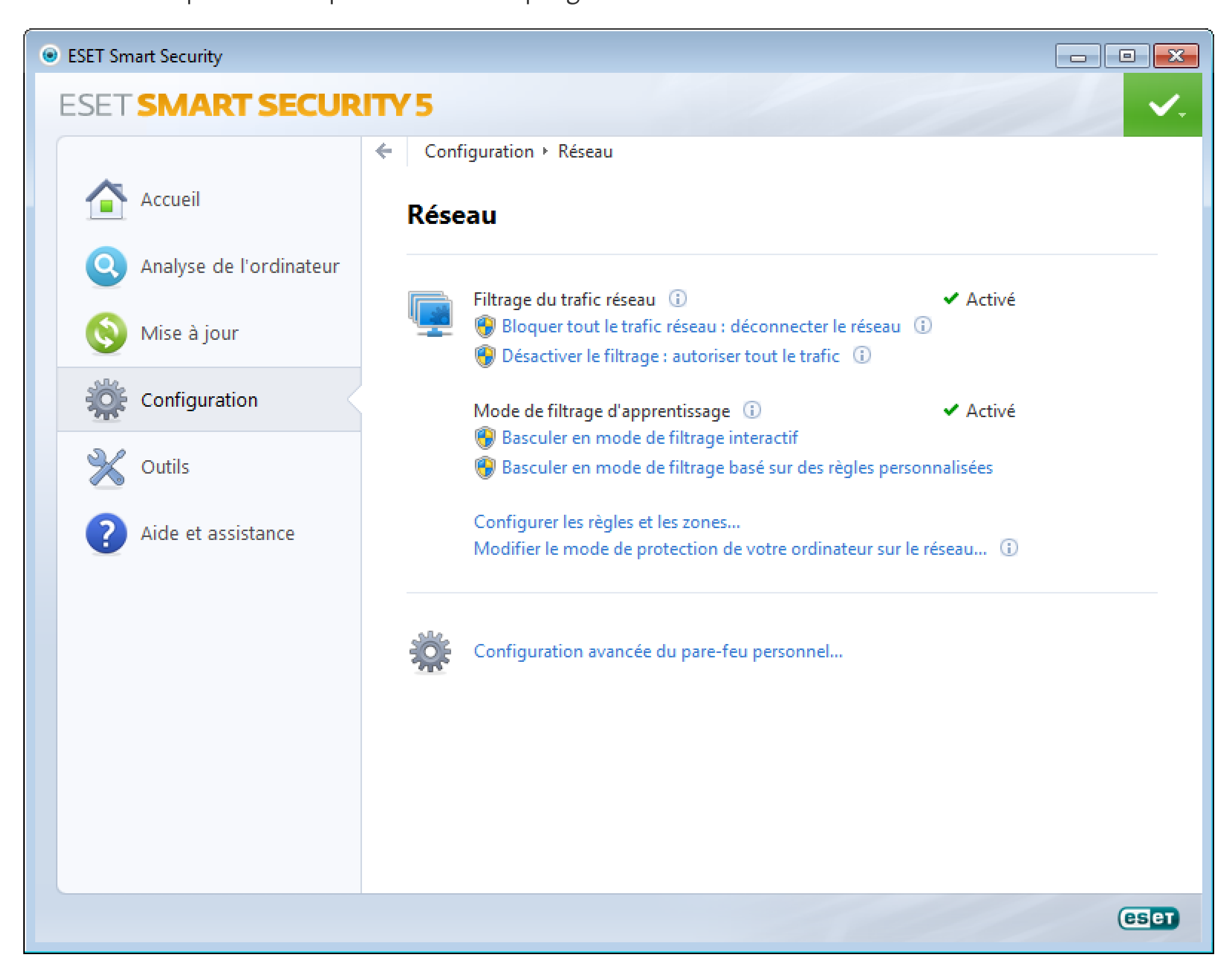
de définir les conditions dans lesquelles autoriser ou refuser cette action. Pour définir les paramètres exacts, cliquez sur **Afficher les options**. Les règles créées de cette manière sont égales aux règles créées manuellement ; la règle créée à partir d'une boîte de dialogue peut être moins spécifique que celle qui a déclenché l'affichage de la boîte de dialogue. En d'autres termes, après la création d'une règle, la même opération peut déclencher la même fenêtre.

L'option **Mémoriser temporairement cette action pour ce processus** provoque la mémorisation de l'action (**Autoriser** / **Refuser**) à utiliser jusqu'à la modification des règles ou du mode de filtrage, une mise à jour du module HIPS ou le redémarrage du système. À l'issue de l'une de ces trois actions, les règles temporaires seront supprimées.

4.2 Réseau

Le pare-feu personnel contrôle tout le trafic réseau entrant et sortant du système. Il autorise ou refuse les différentes connexions réseau en se basant sur les règles de filtrage spécifiées. Il fournit une protection contre les attaques en provenance d'ordinateurs distants et permet de bloquer certains services. Il fournit également une protection antivirus pour les protocoles HTTP, POP3 et IMAP. Cette fonctionnalité représente un élément important de la sécurité d'un ordinateur.

La configuration du pare-feu personnel est disponible dans le volet **Configuration** lorsque vous cliquez sur l'intitulé **Réseau**. Vous pouvez ici régler le mode de filtrage, les règles et les paramètres détaillés. Vous pouvez également accéder à des paramètres plus détaillés du programme.



La seule possibilité pour bloquer tout le trafic réseau consiste à cliquer sur **Bloquer tout le trafic réseau : déconnecter le réseau**. Toutes les communications entrantes et sortantes sont bloquées par le pare-feu personnel. N'utilisez cette option qu'en cas de soupçon de risques critiques de sécurité qui nécessitent la déconnexion du système du réseau.

L'option **Désactiver le filtrage : autoriser tout le trafic** est l'opposé du blocage de l'intégralité du trafic réseau. Si cette option est activée, toutes les options de filtrage du pare-feu personnel sont désactivées et toutes les connexions entrantes et sortantes sont autorisées. C'est comme si le pare-feu personnel n'existait pas. Lorsque le filtrage de trafic réseau est dans l'état **Blocage**, l'option **Basculer en mode de filtrage** active le pare-feu.

Les options suivantes sont disponibles lorsque le mode de filtrage automatique est activé :

- **Mode de filtrage automatique** - Pour modifier le mode de filtrage, cliquez sur l'option **Basculer en mode de filtrage interactif**.
- **Configuration de la zone...** - Affiche les options de configuration de la zone Fiable.

Les options suivantes sont disponibles lorsque le mode de filtrage interactif est activé :

- **Mode de filtrage interactif** - Pour modifier le mode de filtrage, cliquez sur **Basculer en mode de filtrage automatique** ou sur **Basculer en mode de filtrage automatique avec des exceptions** en fonction du mode de filtrage actuel.
- **Configurer les règles et les zones...** - Ouvre la fenêtre **Configuration des zones et des règles** qui vous permet de définir la manière dont le pare-feu gère les communications réseau.

Modifier le mode de protection de votre ordinateur sur le réseau... - Vous pouvez choisir le mode de protection strict ou autorisé.

Configuration avancée du pare-feu personnel... - Permet d'accéder aux options de configuration avancées du pare-feu.

4.2.1 Modes de filtrage

Cinq modes de filtrage sont disponibles pour le pare-feu personnel ESET Smart Security. Les modes de filtrage sont disponibles dans **Configuration avancée** (F5) en cliquant sur **Réseau** > **Pare-feu personnel**. Le comportement du pare-feu change en fonction du mode sélectionné. Les modes de filtrage affectent également le niveau d'interaction de l'utilisateur.

Le filtrage peut être effectué dans l'un des cinq modes :

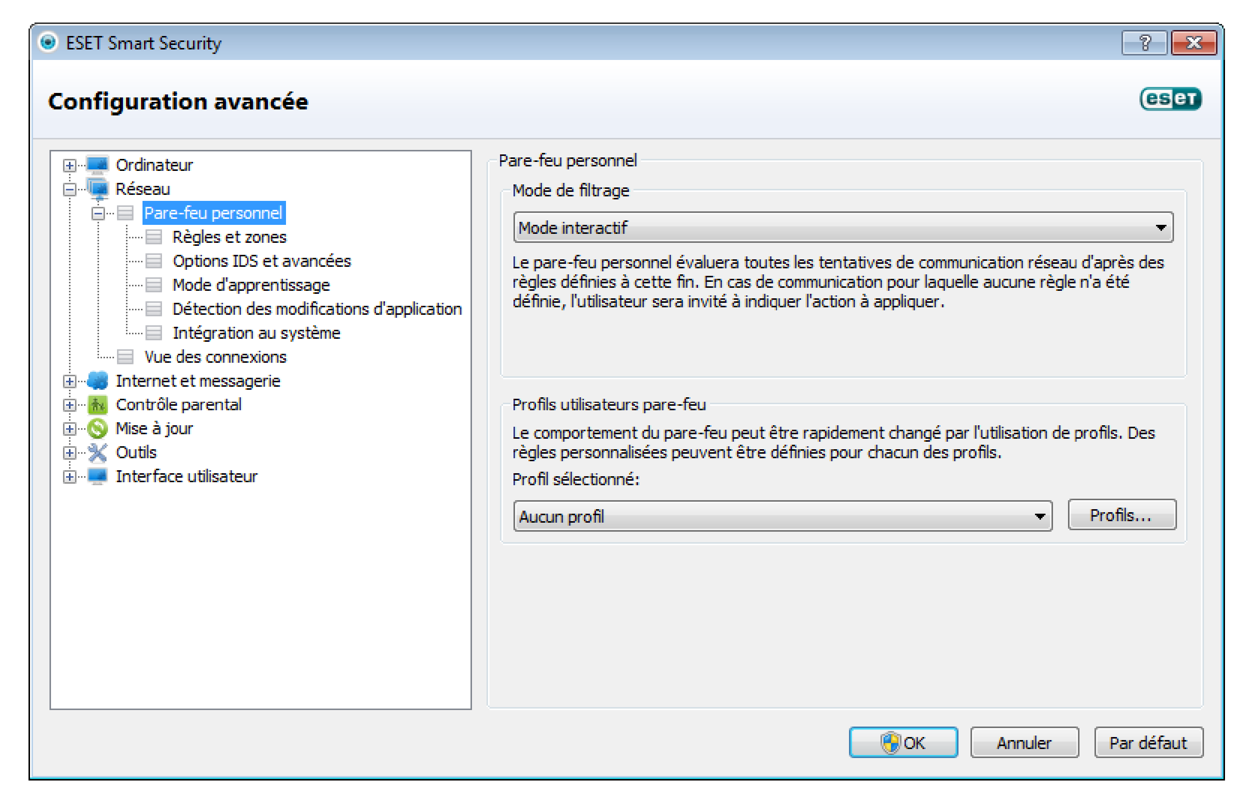
Mode automatique - Mode par défaut. Ce mode convient aux utilisateurs qui préfèrent utiliser le pare-feu simplement, sans définition de règles. Le mode automatique autorise tout trafic sortant du système donné et bloque toutes les nouvelles connexions en provenance du côté distant.

Mode automatique avec exceptions (règles définies par l'utilisateur) - Outre les fonctions du mode automatique, vous pouvez ajouter des règles personnalisées et définies par l'utilisateur.

Mode interactif - Vous permet d'élaborer une configuration personnalisée pour votre pare-feu personnel. Lors de la détection d'une communication à laquelle aucune règle ne s'applique, une boîte de dialogue s'affiche pour signaler une connexion inconnue. Cette boîte de dialogue permet d'autoriser ou de refuser la communication, cette décision pouvant être mémorisée comme nouvelle règle pour le pare-feu personnel. Si vous choisissez de créer une règle à ce moment, toutes les connexions ultérieures de ce type sont autorisées ou refusées, conformément à la règle.

Mode basé sur des règles personnalisées - Le mode basé sur des règles personnalisées bloque toute connexion ne faisant pas l'objet d'une règle spécifique l'autorisant. Ce mode permet aux utilisateurs expérimentés de définir des règles qui n'autorisent que des connexions souhaitées et sûres. Toutes les autres connexions spécifiées sont bloquées par le pare-feu personnel.

Mode d'apprentissage - Crée et enregistre automatiquement les règles ; ce mode convient à la configuration initiale du pare-feu personnel. Aucune intervention de l'utilisateur n'est requise, car ESET Smart Security enregistre les règles conformément aux paramètres prédéfinis. Le mode d'apprentissage n'étant pas sécurisé, il est recommandé de ne l'utiliser que jusqu'à ce que toutes les règles aient été créées pour les communications requises.

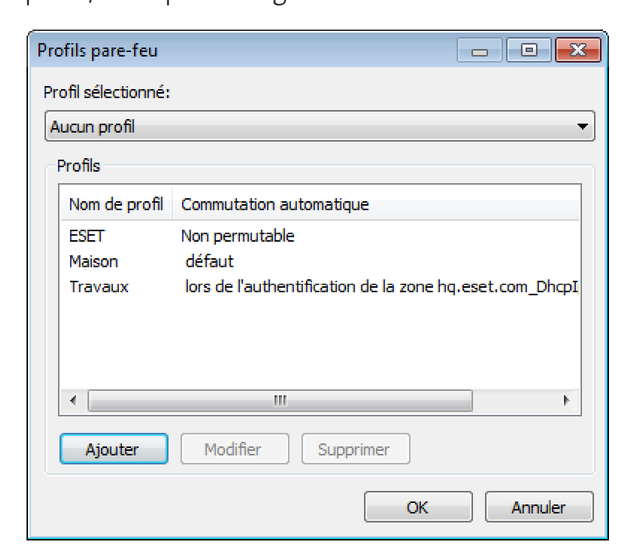


Les Profils permettent de contrôler le comportement du pare-feu personnel ESET Smart Security.

4.2.2 Profils pare-feu

Des profils peuvent être utilisés pour contrôler le comportement du pare-feu personnel de ESET Smart Security. Lorsque vous créez ou modifiez une règle de pare-feu personnel, vous pouvez l'attribuer à un profil spécifique ou l'appliquer à tous les profils. Lorsque vous sélectionnez un profil, seules les règles globales (sans aucun profil indiqué) et les règles attribuées à ce profil sont appliquées. Vous pouvez créer plusieurs profils avec différentes règles attribuées afin de modifier facilement le comportement du pare-feu personnel.

Cliquez sur le bouton **Profils...** (reportez-vous à la section Modes de filtrage) pour ouvrir la fenêtre **Profils pare-feu** dans laquelle vous pouvez **ajouter**, **modifier** ou **supprimer** les profils. Notez que pour **modifier** ou **supprimer** un profil, ce dernier ne doit pas être sélectionné dans le menu déroulant **Profil sélectionné** . Lorsque vous ajoutez ou modifiez un profil, vous pouvez également définir les conditions de son déclenchement.

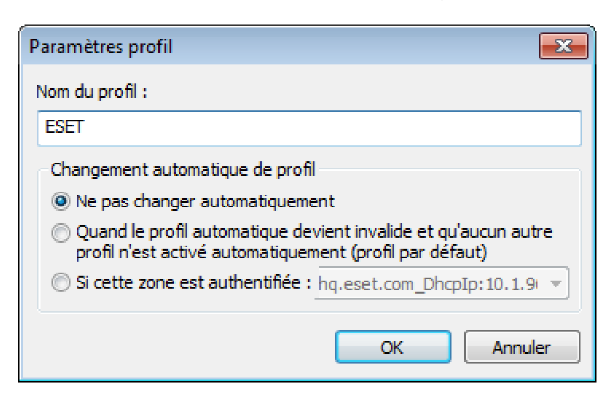


Lorsque vous créez un profil, vous pouvez sélectionner des événements qui vont le déclencher. Les options disponibles sont les suivantes :

- **Ne pas changer automatiquement** - Le déclencheur automatique est désactivé (le profil doit être activé manuellement).
- **Quand le profil automatique devient invalide et qu'aucun autre profil n'est activé automatiquement (profil par défaut)** - Lorsque le profil automatique devient incorrect (si l'ordinateur est connecté à un réseau non fiable, reportez-vous à la section Authentification réseau) et qu'aucun autre profil n'est activé à la place (l'ordinateur n'est pas

connecté à un autre réseau fiable), le pare-feu personnel bascule vers ce profil. Un seul profil peut utiliser ce déclencheur.

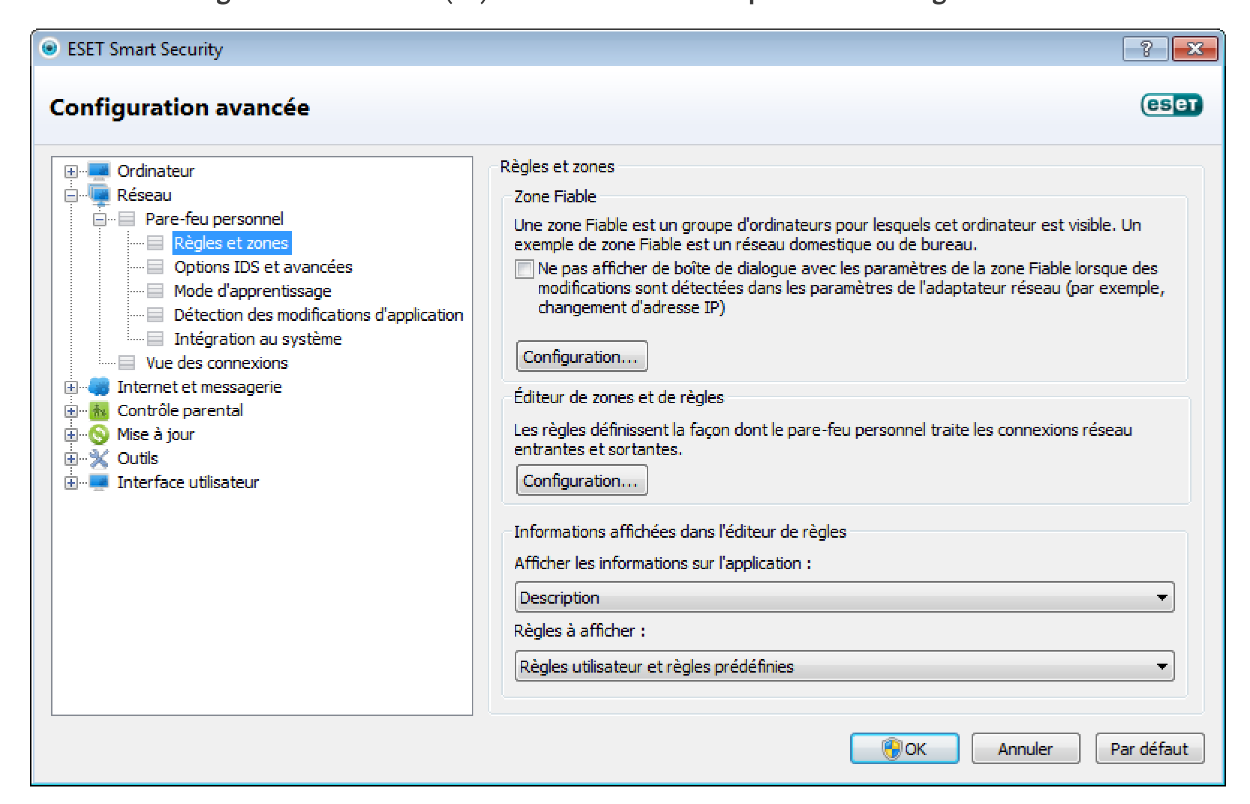
- **Si cette zone est authentifiée** – Ce profil est déclenché lors de l'authentification de la zone spécifiée (reportez-vous à la section Authentification réseau).



Lorsque le pare-feu personnel bascule vers un autre profil, une notification apparaît dans l'angle inférieur droit, à côté de l'horloge système.

4.2.3 Configuration et utilisation des règles

Les règles représentent un ensemble de conditions utilisées pour tester de façon significative toutes les connexions réseau, ainsi que toutes les actions affectées à ces conditions. Avec le pare-feu personnel, vous pouvez définir l'action à entreprendre si une connexion définie par une règle est établie. Pour accéder à la configuration des règles de filtrage, accédez à **Configuration avancée** (F5) > **Réseau** > **Pare-feu personnel** > **Règles et zones**.



Cliquez sur le bouton **Configuration...** de la section **Zone Fiable** pour afficher la fenêtre de configuration de la zone Fiable. L'option **Ne pas afficher de boîte de dialogue avec les paramètres de la zone Fiable...** permet de désactiver l'affichage automatique de la fenêtre de configuration de zone Fiable à chaque détection d'un nouveau sous-réseau. La configuration de zones actuelle est automatiquement utilisée.

REMARQUE : si le pare-feu personnel est défini sur **Mode automatique**, certains paramètres ne sont pas disponibles.

Cliquez sur le bouton Configuration... de la section **Éditeur de zones et de règles** pour afficher la fenêtre **Configuration des zones et des règles** qui présente les règles ou les zones (en fonction de l'onglet sélectionné). La fenêtre est divisée en deux sections. La section supérieure donne un aperçu résumé de chaque règle. La section inférieure affiche les détails de la règle sélectionnée dans la section supérieure. Les boutons **Nouveau**, **Modifier** et **Supprimer**, disponibles dans la partie inférieure de la fenêtre, vous permettent de configurer les règles.

Les connexions peuvent être divisées en connexions entrantes et sortantes. Les connexions entrantes sont initiées par un ordinateur distant qui tente d'établir une connexion avec le système local. Les connexions sortantes fonctionnent dans le sens opposé : le côté local contacte l'ordinateur distant.

Si une nouvelle communication inconnue est détectée, la décision de l'autoriser ou de la rejeter doit être prise avec prudence. Les connexions non sollicitées, non sécurisées ou inconnues posent un risque de sécurité au système. Si une telle connexion est établie, il est recommandé de faire très attention au côté distant et aux applications qui tentent de se connecter à votre ordinateur. De nombreuses infiltrations essaient d'obtenir et d'envoyer des données personnelles ou de télécharger d'autres applications malveillantes aux postes de travail hôtes. Le pare-feu personnel permet à l'utilisateur de détecter et de mettre fin à de telles connexions.

L'option **Afficher les informations sur l'application** permet de définir la façon dont les applications sont affichées dans la liste de règles. Les options disponibles sont les suivantes :

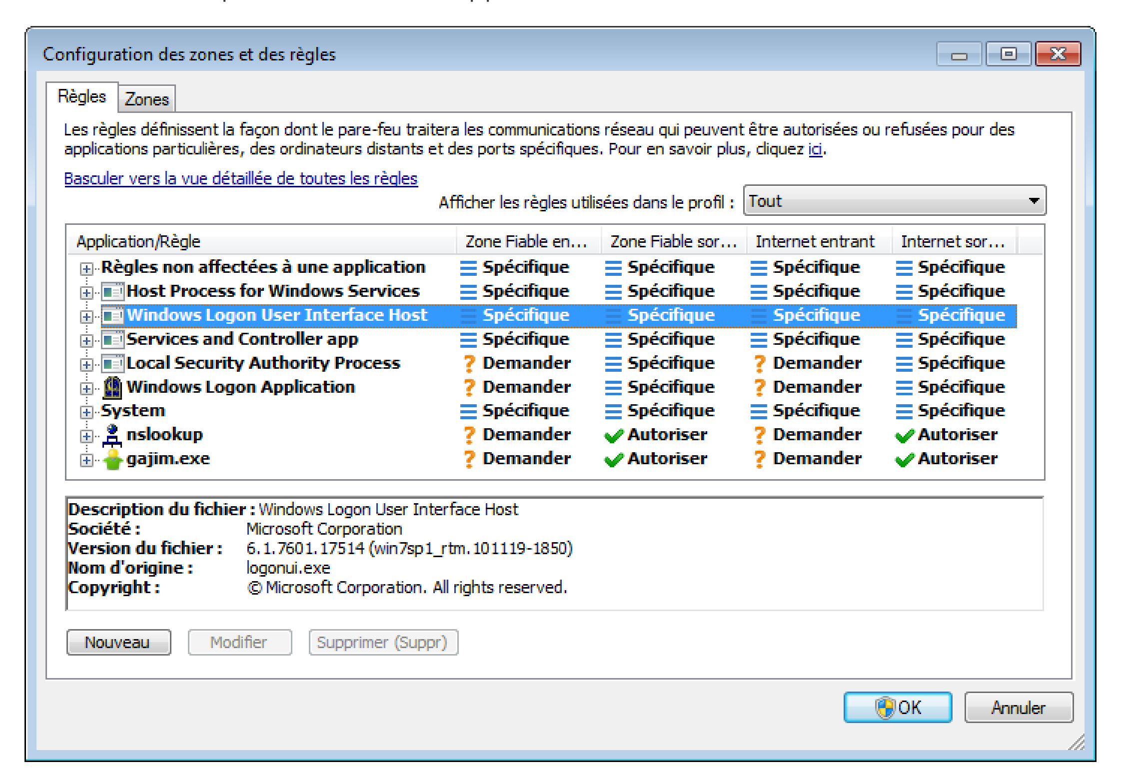
- **Chemin complet** - Chemin d'accès complet à l'exécutable de l'application.
- **Description** - Description de l'application.
- **Nom** - Nom de l'exécutable de l'application.

Sélectionnez le type de règles qui apparaissent dans la liste **Règles à afficher** :

- **Uniquement les règles définies par l'utilisateur** - Affiche uniquement les règles créées par l'utilisateur.
- **Règles utilisateur et règles prédéfinies** - Affiche toutes les règles définies par l'utilisateur et les règles par défaut prédéfinies.
- **Toutes les règles (y compris système)** - Affiche toutes les règles.

4.2.3.1 Configuration des règles

La configuration des règles permet de voir toutes les règles appliquées au trafic généré par des applications dans des zones fiables et sur Internet. Par défaut, des règles sont automatiquement ajoutées en fonction des réactions de l'utilisateur à une nouvelle communication. Pour afficher des informations supplémentaires sur l'application au bas de cette fenêtre, cliquez sur le nom de l'application.



Chaque ligne correspondant à une règle commence par un bouton qui permet de développer/réduire (+/-) les informations. Dans la colonne **Application/Règle**, cliquez sur le nom de l'application pour afficher des informations sur la règle au bas de cette fenêtre. Le menu contextuel permet de modifier le mode d'affichage. Vous pouvez également utiliser le menu contextuel pour ajouter, modifier et supprimer des règles.

Zone Fiable entrante/Zone Fiable sortante - Actions liées à la communication entrante et sortante de la zone Fiable.

Internet entrant/Internet sortant - Actions liées aux connexions Internet et concernant la communication entrante ou sortante.

Pour chaque type (sens) de communication, vous pouvez sélectionner les actions suivantes :

- ✔ **Autoriser** - Pour autoriser les communications.
- ? **Demander** - Vous être invité à autoriser ou à refuser la communication chaque fois qu'elle est établie.
- ✖ **Refuser** - Pour refuser les communications.
- ☰ **Spécifique** - Ne peut pas être classé en fonction des autres actions. Par exemple, si une adresse IP ou un port spécifique a été autorisé par le pare-feu personnel, cette information ne peut pas être classée avec certitude si les communications entrantes ou sortantes sont autorisées.

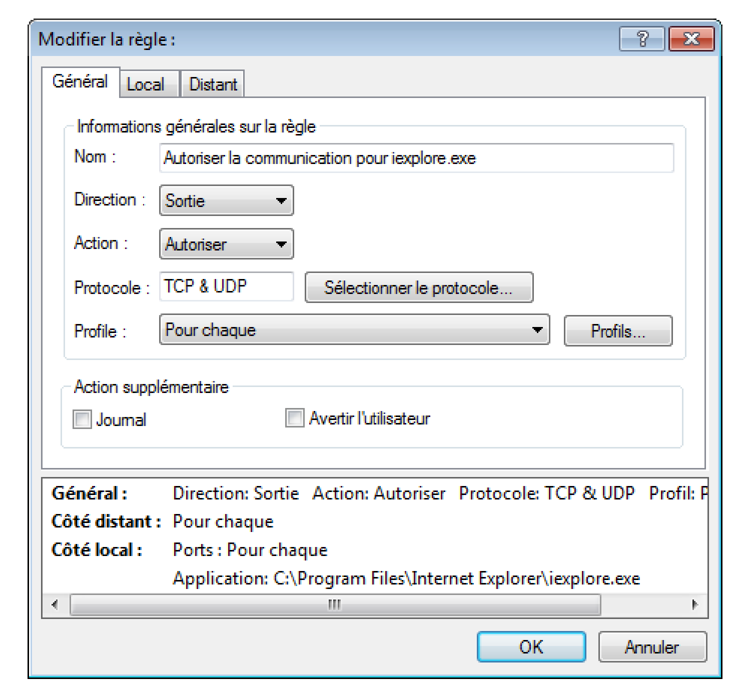
Une nouvelle règle doit être créée à chaque installation de nouvelle application accessible au réseau, ou en cas de modification de connexion existante (côté distant, numéro de port, etc.). Pour modifier une règle existante, vérifiez que l'onglet **Règles** est sélectionné et cliquez sur le bouton **Modifier**.

4.2.3.2 Modification des règles

Une modification s'impose chaque fois qu'un paramètre de contrôle change. Dans ce cas, la règle ne peut pas remplir les conditions et ses actions prédéfinies ne peuvent pas être appliquées. Si les paramètres sont modifiés, la connexion risque d'être refusée et cela peut engendrer des problèmes de fonctionnement de l'application en question. Un exemple est le changement d'adresse ou le numéro de port du côté distant.

La partie supérieure de la fenêtre contient trois onglets :

- **Général** - Spécifie un nom de règle, le sens de la connexion, l'action, le protocole et le profil auquel la règle s'applique.
- **Local** - Affiche les informations concernant la partie locale de la connexion, notamment le numéro du port local ou la plage des ports, ainsi que le nom de l'application communicante.
- **Distant** - Cet onglet comprend des informations concernant le port distant (plage de ports). Il vous permet également de définir la liste des adresses IP ou zones distantes pour la règle en question.



Protocole représente le protocole de transfert utilisée par la règle. Cliquez sur **Sélectionner le protocole...** pour ouvrir la fenêtre Sélection du protocole.

Par défaut, toutes les règles sont activées **Pour chaque** profil. Vous pouvez également sélectionner un profil de pare-feu personnalisé à l'aide du bouton **Profils...**.

Si vous cliquez sur **Journal**, l'activité liée à la règle est enregistrée dans un journal. L'option **Notifier l'utilisateur** affiche une notification lorsque la règle est appliquée.

La zone d'informations récapitule la règle en bas des trois onglets. Vous verrez les mêmes informations si vous cliquez sur la règle dans la fenêtre principale (**Outils** > **Connexions réseau** ; cliquez avec le bouton droit sur la règle et activez l'option **Afficher les détails** (reportez-vous à la section Connexions réseau)).

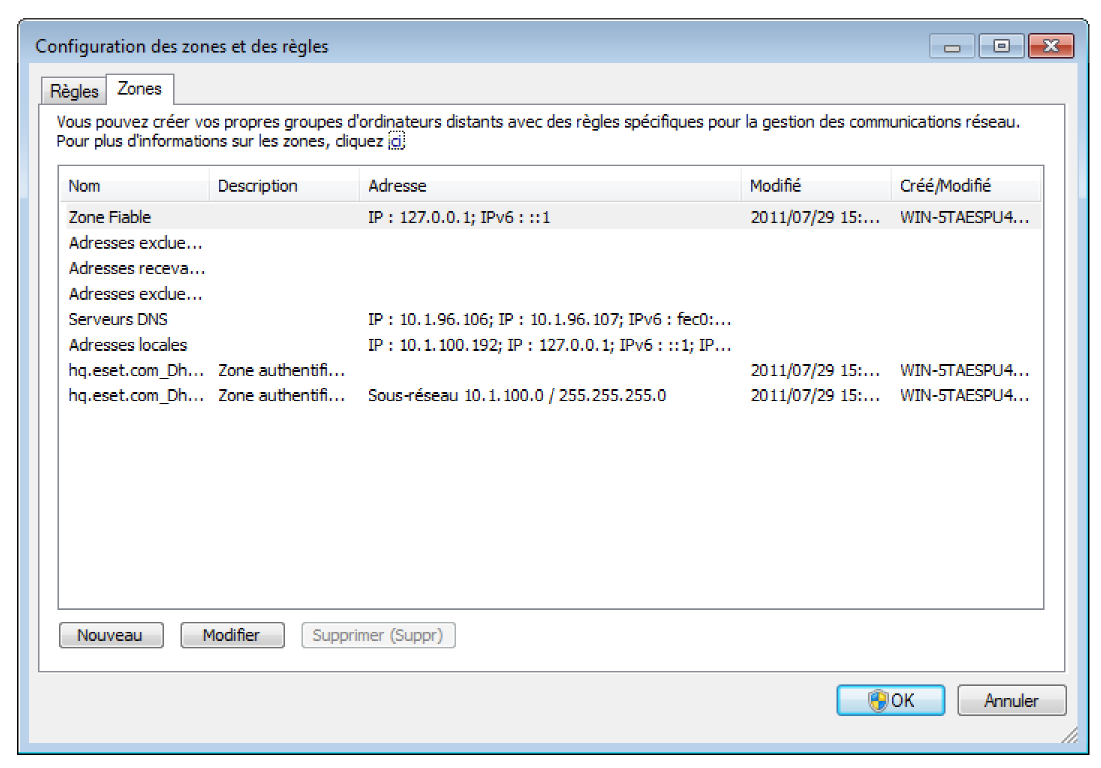
Lorsque vous créez une règle, vous devez entrer son nom dans le champ **Nom**. Sélectionnez le sens dans lequel la règle s'applique dans le menu déroulant **Direction**. Définissez l'action à exécuter lorsqu'une communication rencontre la règle, à partir du menu déroulant **Action**.

Un bon exemple d'ajout de nouvelle règle consiste à autoriser le navigateur Internet à accéder au réseau. Dans ce cas, les informations suivantes doivent être fournies :

- Dans l'onglet **Général**, activez les communications sortantes via les protocoles TCP et UDP.
- Ajoutez le processus représentant le navigateur (pour Internet Explorer, iexplore.exe) dans l'onglet **Local**.
- Dans l'onglet **Distant**, activez le port numéro 80 pour n'autoriser que la navigation Internet standard.

4.2.4 Configuration des zones

Dans la fenêtre **Configuration de la zone**, vous pouvez indiquer le nom de la zone, la description, la liste des adresses réseau et l'authentification de la zone (consultez la section Authentification de zone - Configuration du client).



Les zones représentent des groupes d'adresses réseau constituant un groupe logique. Chaque adresse d'un groupe donné reçoit les mêmes règles que celles définies au niveau global du groupe. La **zone Fiable** est un exemple de groupe. La zone Fiable représente un groupe d'adresses réseau qui sont totalement fiables et qui ne sont pas bloquées par le pare-feu personnel.

Ces zones peuvent être configurées au moyen de l'onglet **Zones** de la fenêtre **Configuration des zones et des règles**, en cliquant sur le bouton **Modifier**. Saisissez un **nom** pour la zone et une **description**, puis ajouter une adresse IP distante en cliquant sur le bouton **Ajouter une adresse IPv4/IP6**.

4.2.4.1 Authentification réseau

Pour les ordinateurs portables, il est recommandé de vérifier la fiabilité du réseau auquel vous vous connectez. La zone Fiable est identifiée par l'adresse IP locale de l'adaptateur réseau. Les ordinateurs portables se connectent souvent à des réseaux avec des adresses IP semblables à celle du réseau fiable. Si les paramètres de zone Fiable ne sont pas basculés automatiquement sur **Protection stricte**, le pare-feu personnel continue à utiliser le mode **Autoriser le partage**.

Pour éviter ce genre de situation, il est recommandé d'utiliser l'authentification de zone.

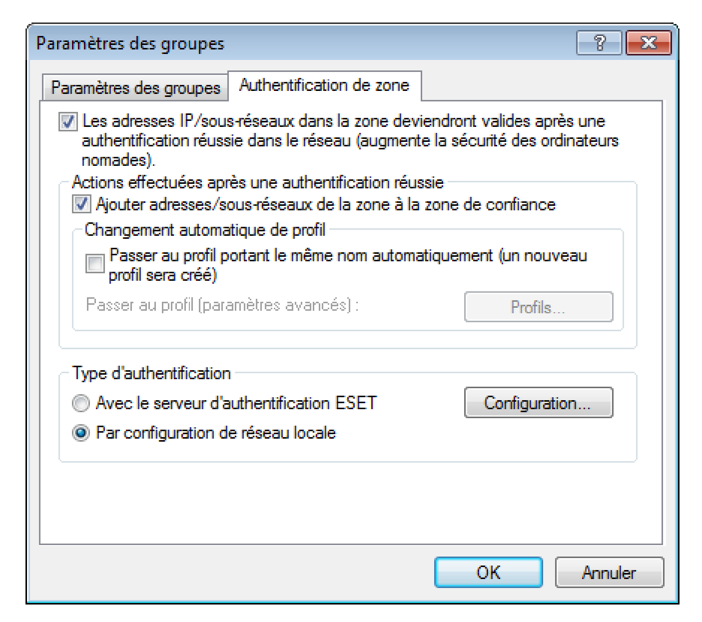
4.2.4.1.1 Authentification de zone - Configuration du client

Dans la fenêtre **Configuration des zones et des règles**, cliquez sur l'onglet **Zones** et créez une zone à l'aide du nom de la zone authentifiée par le serveur. Cliquez ensuite sur **Ajouter une adresse IPv4** et sélectionnez l'option **Sous-réseau** pour ajouter un masque de sous-réseau contenant le serveur d'authentification.

Cliquez sur l'onglet **Authentification de zone**. Chaque zone peut être définie pour s'authentifier sur le serveur. La zone (son adresse IP et le sous-réseau) sont valides après leur authentification. Par exemple, les actions telles que l'accès au profil de pare-feu et l'ajout d'une adresse/d'un sous-réseau de la zone à la zone Fiable ne sont effectuées qu'après l'authentification.

Sélectionnez l'option **Les adresses IP/sous-réseaux de la zone deviendront valides...** pour que la zone devienne non valide si l'authentification n'aboutit pas. Pour sélectionner un profil de pare-feu personnel après l'authentification réussie d'une zone, cliquez sur le bouton **Profils...**

Si vous sélectionnez l'option **Ajouter adresses/sous-réseaux de la zone à la zone de confiance**, les adresses/sous-réseaux de la zone sont ajoutés à la zone Fiable après l'authentification (recommandé). Si l'authentification n'aboutit pas, les adresses ne sont pas ajoutées à la zone Fiable. Si l'option **Passer au profil portant le même nom automatiquement (un nouveau profil sera créé)** est active, le nouveau profil est créé une fois l'authentification effectuée correctement. Cliquez sur le bouton **Profils...** pour ouvrir la fenêtre Profils pare-feu.



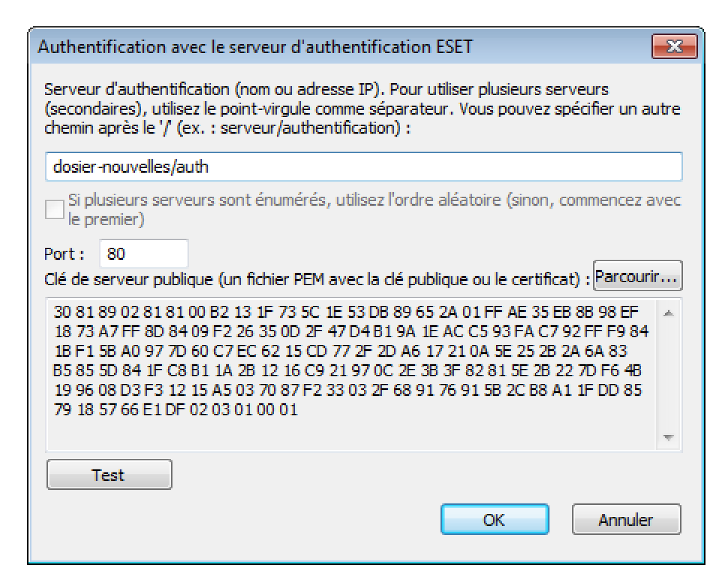
Il existe deux types d'authentification :

1) Utilisation du serveur d'authentification ESET

L'authentification de zone recherche un serveur spécifique sur le réseau et utilise le chiffrement asymétrique (algorithme RAS) pour authentifier le serveur. L'authentification est répétée pour chaque réseau auquel votre ordinateur se connecte. Cliquez sur **Configuration...** et indiquez un nom de serveur, un port d'écoute de serveur et une clé publique correspondant à la clé privée du serveur (reportez-vous à la section Authentification de zone - Configuration du serveur). Le nom du serveur peut être saisi sous la forme d'une adresse IP, ou d'un nom DNS ou NetBios. Le nom du serveur peut être suivi d'un chemin indiquant l'emplacement de la clé sur le serveur (par exemple *nom_serveur/répertoire1/répertoire2/authentification*). Saisissez plusieurs serveurs, séparés par des points-virgules ; ils seront utilisés si le premier serveur n'est pas disponible.

La clé publique peut être un fichier de l'un des types suivants :

- Clé publique chiffrée PEM (.pem)
  Cette clé peut être générée à l'aide du serveur d'authentification ESET (reportez-vous à la section Authentification de zone - Configuration du serveur).
- Clé publique chiffrée
- Certificat de clé publique (.crt)



Pour tester vos paramètres, cliquez sur le bouton **Test**. Si l'authentification aboutit, le message *Authentification de serveur réussie* apparaît. Si l'authentification n'est pas configurée correctement, l'un des messages d'erreur suivants apparaît :

Authentification de serveur échouée. Le temps maximum pour l'authentification s'est écoulé.
Le serveur d'authentification est inaccessible. Vérifiez le nom du serveur/l'adresse IP et/ou vérifiez les paramètres de pare-feu personnel du client, ainsi que la partie serveur.

Une erreur s'est produite lors de la communication avec le serveur.
Le serveur d'authentification n'est pas en cours d'exécution. Démarrez le service du serveur d'authentification (reportez-vous à la section Authentification de zone - Configuration du serveur).

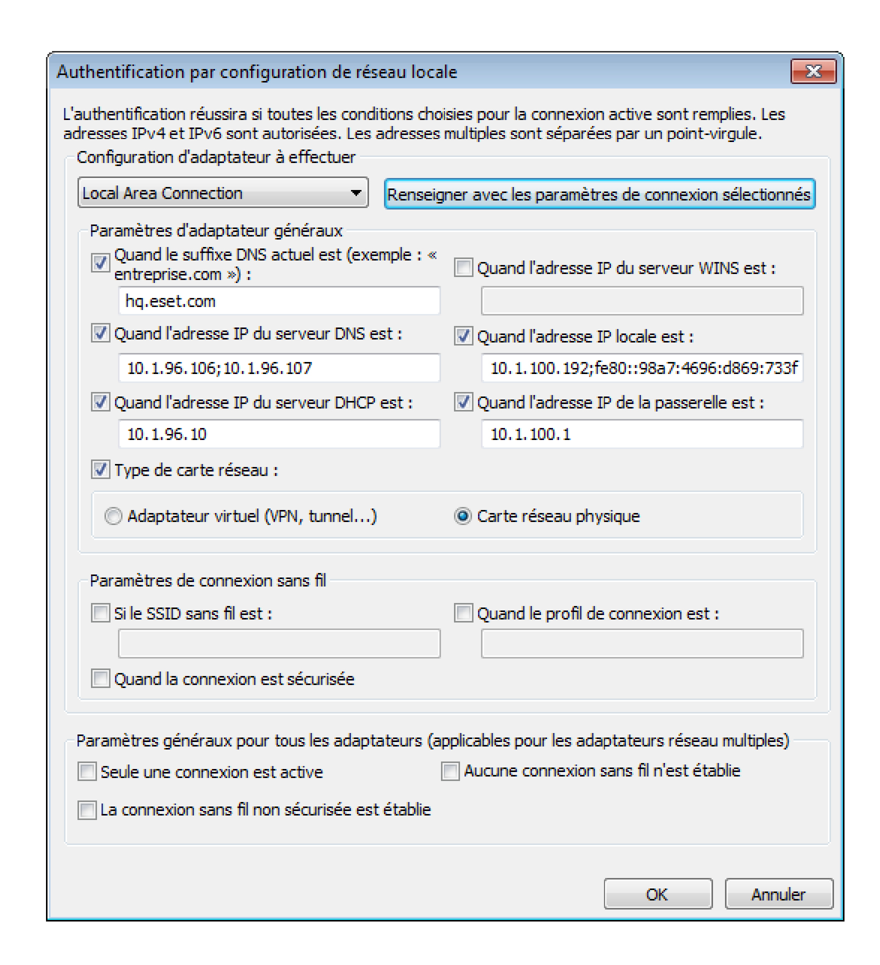
Le nom de la zone d'authentification ne correspond pas à la zone de serveur.
Le nom de la zone configurée ne correspond pas à la zone du serveur d'authentification. Examinez les deux zones et vérifiez que les noms sont identiques.

Authentification de serveur échouée. Adresse de serveur non trouvée dans la liste d'adresses pour la zone donnée.
L'adresse IP de l'ordinateur qui exécute le serveur d'authentification est en dehors de la plage d'adresses IP définie pour la configuration actuelle de la zone.

Authentification de serveur échouée. Une clé publique non valide a probablement été entrée.
Vérifiez que la clé publique indiquée correspond à la clé privée du serveur. Vérifiez également que le fichier de clé publique n'est pas endommagé.

2) Par configuration de réseau locale

L'authentification est effectuée en fonction des paramètres d'une carte de réseau local. La zone est authentifiée si tous les paramètres sélectionnés pour la connexion active sont corrects.



4.2.4.1.2 Authentification de zone - Configuration du serveur

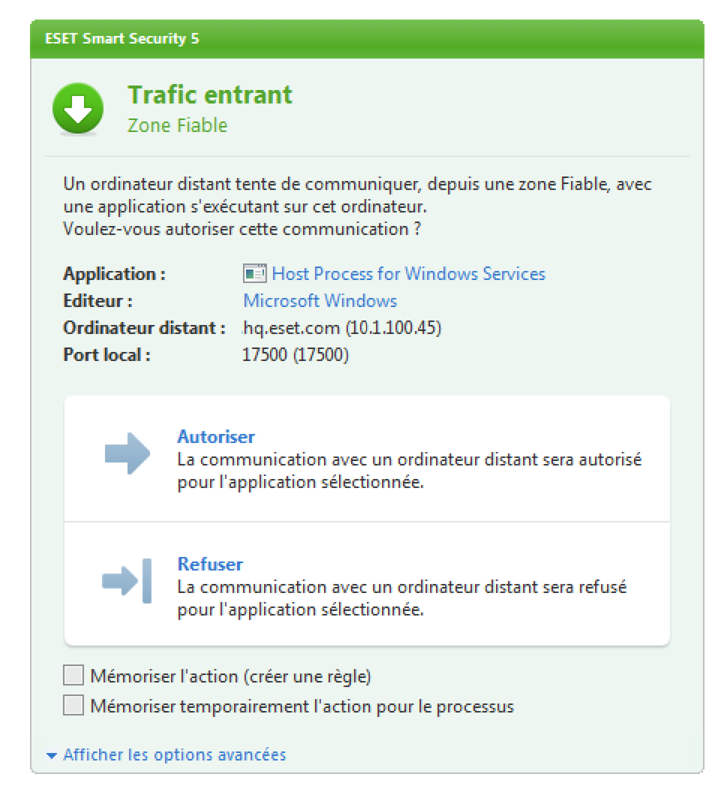
Le processus d'authentification peut être exécuté par tout ordinateur/serveur connecté au réseau et qui doit être authentifié. L'application ESET Authentication Server doit être installée sur un ordinateur/serveur qui est toujours accessible pour l'authentification dès qu'un client tente de se connecter au réseau. Le fichier d'installation de l'application ESET Authentication Server est téléchargeable depuis le site ESET.

Après l'installation de l'application ESET Authentication Server, une boîte de dialogue apparaît (vous pouvez accéder à l'application à tout moment en cliquant sur **Démarrer** > **Programmes** > **ESET** > **ESET Authentication Server**).

Pour configurer le serveur d'authentification, saisissez le nom de la zone d'authentification, le port d'écoute du serveur (il s'agit par défaut du port 80), ainsi que l'emplacement de stockage de la paire clé publique-clé privée. Générez ensuite la clé publique et la clé privée qui seront utilisées dans l'authentification. La clé privée reste sur le serveur, tandis que la clé publique doit être importée sur le client, dans la section d'authentification de zone, lors de la configuration d'une zone de la configuration du pare-feu.

4.2.5 Établissement d'une connexion - détection

Le pare-feu personnel détecte toute nouvelle connexion au réseau. Le mode pare-feu actif détermine les actions à exécuter pour la nouvelle règle. Si l'option **Mode automatique** ou **Mode basé sur des règles personnalisées** est activée, le pare-feu personnel exécutera les actions prédéfinies sans intervention de l'utilisateur. Le mode interactif affiche une fenêtre d'information qui signale la détection d'une nouvelle connexion réseau et donne des informations détaillées sur la connexion. Vous pouvez choisir d'autoriser la connexion ou de la refuser (la bloquer). Si vous autorisez toujours la même connexion dans la boîte de dialogue, il est recommandé de créer une nouvelle règle pour la connexion. Pour ce faire, sélectionnez l'option **Mémoriser l'action (créer une règle)** et sauvegardez l'action comme une nouvelle règle pour le pare-feu personnel. Si le pare-feu personnel reconnaît ultérieurement cette connexion, il applique la règle existante sans intervention de l'utilisateur.



Soyez très attentif lors de la création de nouvelles règles. Pensez également à n'autoriser que les connexions sécurisées. Si toutes les connexions sont autorisées, le pare-feu personnel n'a aucune raison d'exister. Voici les paramètres importants pour les connexions :

- **Côté distant** - Autorise uniquement les connexions aux adresses fiables et connues.
- **Application locale** - Il n'est pas conseillé d'autoriser la connexion d'applications et processus inconnus.
- **Numéro de port** - Les communications via les ports communs (le port 80 pour le trafic Internet par exemple) doivent toujours être autorisées en situation normale.

Pour proliférer, les infiltrations dans les ordinateurs utilisent souvent des connexions masquées et Internet pour infecter les systèmes distants. Si les règles sont correctement configurées, le pare-feu personnel devient un important outil de protection contre les diverses attaques répétées des codes malveillants.

4.2.6 Journalisation

Le pare-feu personnel ESET Smart Security enregistre tous les événements importants dans un journal, accessible directement à partir du menu du programme. Cliquez sur **Outils** > **Fichiers journaux**, puis sélectionnez **Journal du pare-feu ESET** dans le menu déroulant **Journal**.

Les fichiers journaux sont un outil inestimable pour la détection des erreurs et la révélation des intrusions dans le système. Le journal du pare-feu personnel d'ESET contient les données suivantes :

- Date et heure de l'événement
- Nom de l'événement
- Source
- Adresse réseau cible
- Protocole de communication réseau
- Règle appliquée ou nom du ver s'il est identifié
- Application concernée
- Utilisateur

Une analyse approfondie de ces données peut contribuer à détecter les tentatives qui risquent de compromettre la sécurité du système. Beaucoup d'autres facteurs peuvent informer l'utilisateur sur les risques potentiels de sécurité et l'aident à minimiser leur effet : trop de connexions en provenance de sites inconnus, plusieurs tentatives d'établissement de connexions, communications issues d'applications inconnues, utilisation de numéros de ports inhabituels.

4.2.7 Intégration au système

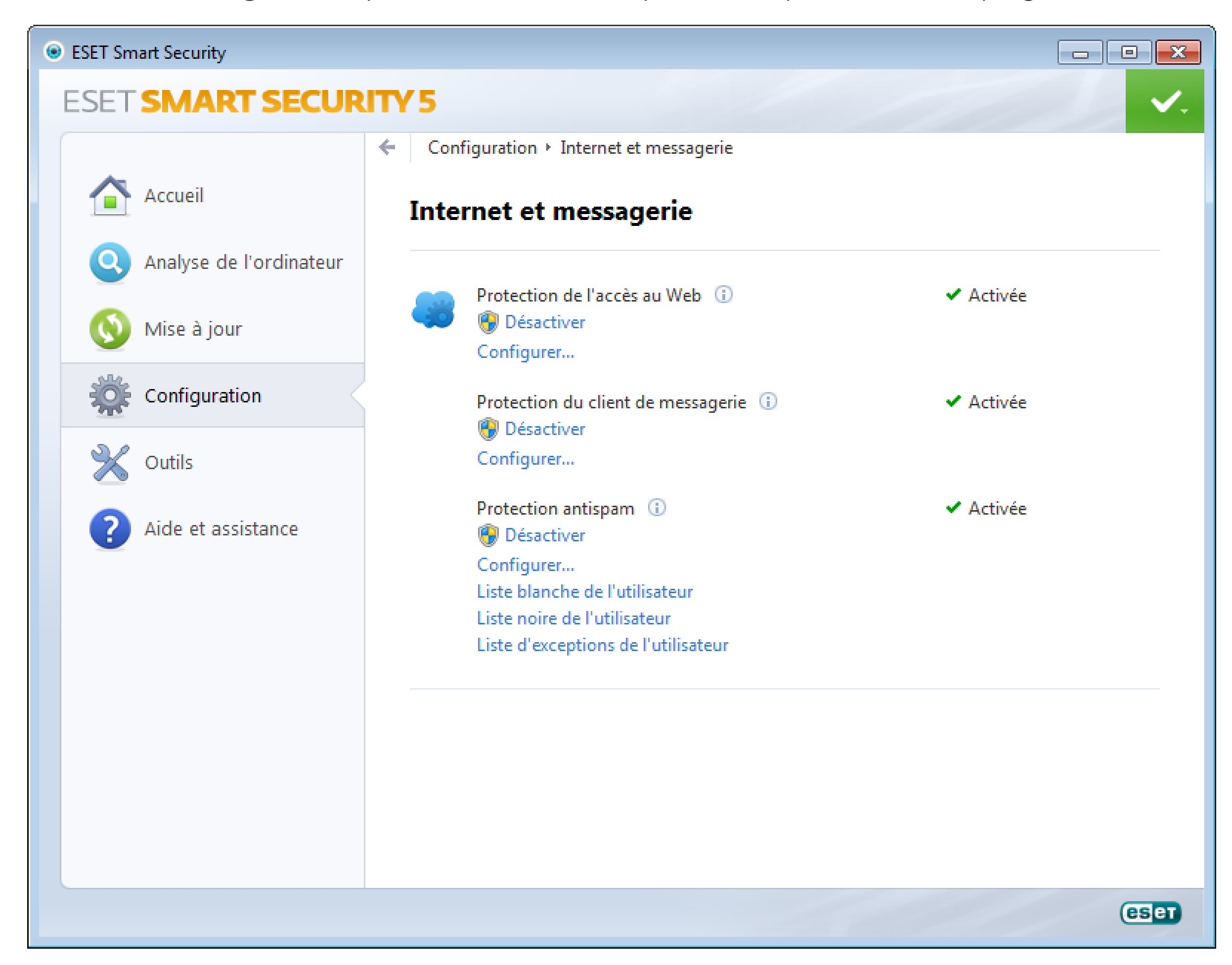
Le pare-feu personnel d'ESET Smart Security peut opérer à plusieurs niveaux :

- **Toutes les fonctions actives** - Le pare-feu personnel est totalement intégré et ses composants sont actifs (option par défaut). Si l'ordinateur est connecté à un réseau de grande taille ou à Internet, il est conseillé de laisser cette option activée. Cette option est la plus sûre et elle protège complètement votre système.
- **Pare-feu personnel inactif** - Le pare-feu personnel est intégré dans le système, il sert d'intermédiaire pour les communications réseau, mais ne recherche pas les menaces.
- **N'analyser que les protocoles d'application** - Seuls les composants du pare-feu personnel assurant l'analyse des protocoles d'application (HTTP, POP3, IMAP et leur version sécurisée) sont actifs. Si les protocoles d'application ne sont pas analysés, la protection est effectuée au niveau de la protection en temps réel du système et de l'analyse à la demande de l'ordinateur.
- **Le pare-feu personnel est complètement désactivé** - Activez cette option pour désactiver totalement le pare-feu personnel du système. Aucune analyse n'est effectuée. Cette option peut être utile pour effectuer un test. Lorsqu'une application est bloquée, vous pouvez vérifier si elle est bloquée par le pare-feu. Cette option est la moins sûre ; il est donc recommandé de procéder avec prudence lors de la désactivation totale du pare-feu.

Différer la mise à jour du module de pare-feu personnel jusqu'à un redémarrage de l'ordinateur - La mise à jour est simplement téléchargée ; l'installation est effectuée au redémarrage de l'ordinateur.

4.3 Internet et messagerie

La configuration d'Internet et messagerie est disponible dans le volet **Configuration** lorsque vous cliquez sur l'intitulé **Internet et messagerie**. Elle permet d'accéder à des paramètres plus détaillés du programme.



La connectivité Internet est une fonctionnalité standard des ordinateurs personnels. Elle est malheureusement devenue le principal mode de transfert des codes malveillants. Il est donc essentiel de surveiller de près la **Protection de l'accès au Web et antihameçonnage**.

Protection du client de messagerie - Offre le contrôle de la communication par courrier électronique effectuée via les protocoles POP3 et IMAP. ESET Smart Security utilise le plugin de votre client de messagerie pour contrôler toutes les communications concernant le client de messagerie (POP3, MAPI, IMAP, HTTP).

La **protection antispam** filtre les messages non sollicités.

Désactiver - Désactive la protection Internet/de messagerie/antispam des clients de messagerie.

Configurer... - Ouvre les paramètres avancés de protection Internet/de messagerie/antispam .

Liste blanche de l'utilisateur - Ouvre une boîte de dialogue permettant d'ajouter, de modifier ou de supprimer des adresses de messagerie considérées comme étant sûres. Les messages dont l'adresse de l'expéditeur est répertoriée dans la liste blanche ne font pas l'objet d'une analyse de courrier indésirable.

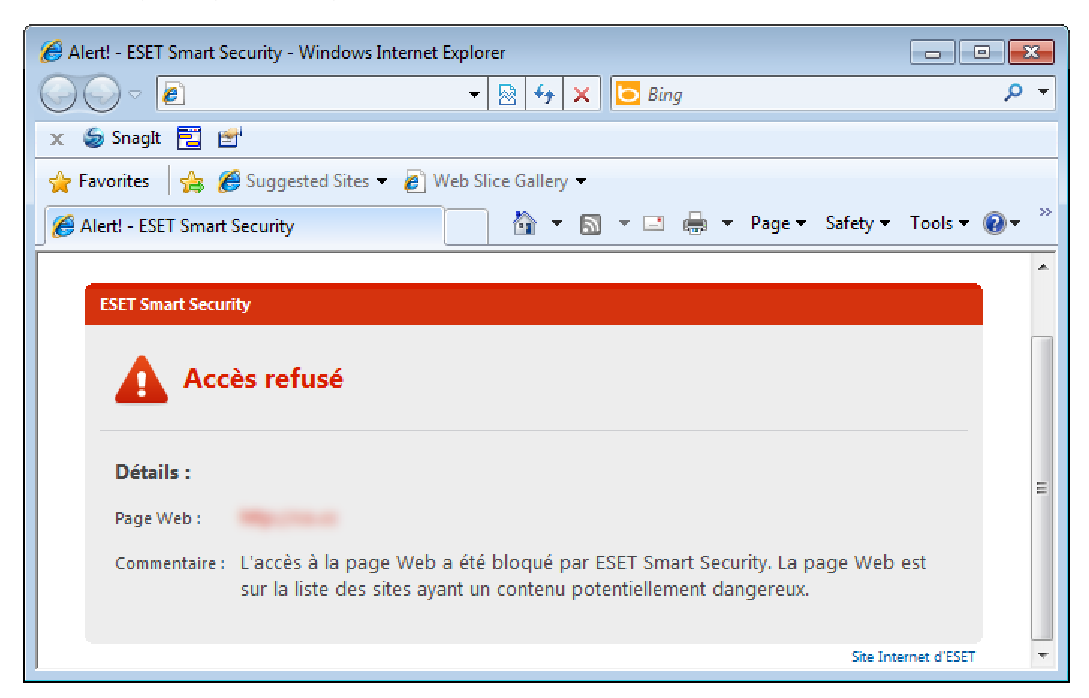
Liste noire de l'utilisateur - Ouvre une boîte de dialogue permettant d'ajouter, de modifier ou de supprimer des adresses de messagerie considérées comme étant potentiellement dangereuses. Les messages dont l'adresse de l'expéditeur est répertoriée dans la liste noire sont considérés comme du courrier indésirable.

Liste d'exceptions de l'utilisateur - Ouvre une boîte de dialogue permettant d'ajouter, de modifier ou de supprimer des adresses de messagerie qui peuvent être usurpées et utilisées pour l'envoi de courrier indésirable. Les messages dont l'adresse de l'expéditeur est répertoriée dans la liste d'exception font toujours l'objet d'une analyse de courrier indésirable. Par défaut, la liste d'exception contient vos adresses de messagerie figurant dans les comptes de client de messagerie existants.

4.3.1 Protection de l'accès au Web et antihameçonnage

La connectivité Internet est une fonctionnalité standard des ordinateurs personnels. Elle est malheureusement devenue le principal mode de transfert des codes malveillants. Protection de l'accès au Web et antihameçonnage opère par surveillance des communications entre les navigateurs Internet et les serveurs distants, conformément aux règles des protocoles HTTP et HTTPS (communications chiffrées).

Le terme d'hameçonnage (phishing en anglais) désigne une activité frauduleuse utilisant des techniques de piratage psychologique qui consistent à manipuler les utilisateurs pour obtenir des informations confidentielles. Pour en savoir plus sur cette activité, reportez-vous au glossaire. ESET Smart Security prend en charge la protection antihameçonnage ; les pages Web connues qui présentent ce type de contenu sont toujours bloquées.



Nous vous recommandons vivement d'activer l'option Protection de l'accès au Web et antihameçonnage . Cette option est accessible depuis la fenêtre principale de ESET Smart Security en naviguant vers **Configuration** > **Internet et messagerie** > **Protection de l'accès au Web et antihameçonnage**.

4.3.1.1 HTTP, HTTPs

Par défaut, ESET Smart Security est configuré pour utiliser les normes de la plupart des navigateurs Internet. Toutefois, vous pouvez modifier les options de configuration de l'analyseur HTTP dans la section **Configuration avancée** (F5) > **Internet et messagerie** > **Protection de l'accès au Web et antihameçonnage** > **HTTP, HTTPS**. Dans la fenêtre principale du **filtre HTTP**, vous pouvez activer ou désactiver l'option **Activer le contrôle HTTP**. Vous pouvez également définir les numéros de port utilisés pour la communication HTTP. Par défaut, les numéros de ports 80 (HTTP), 8080 et 3128 (pour le serveur proxy) sont prédéfinis.

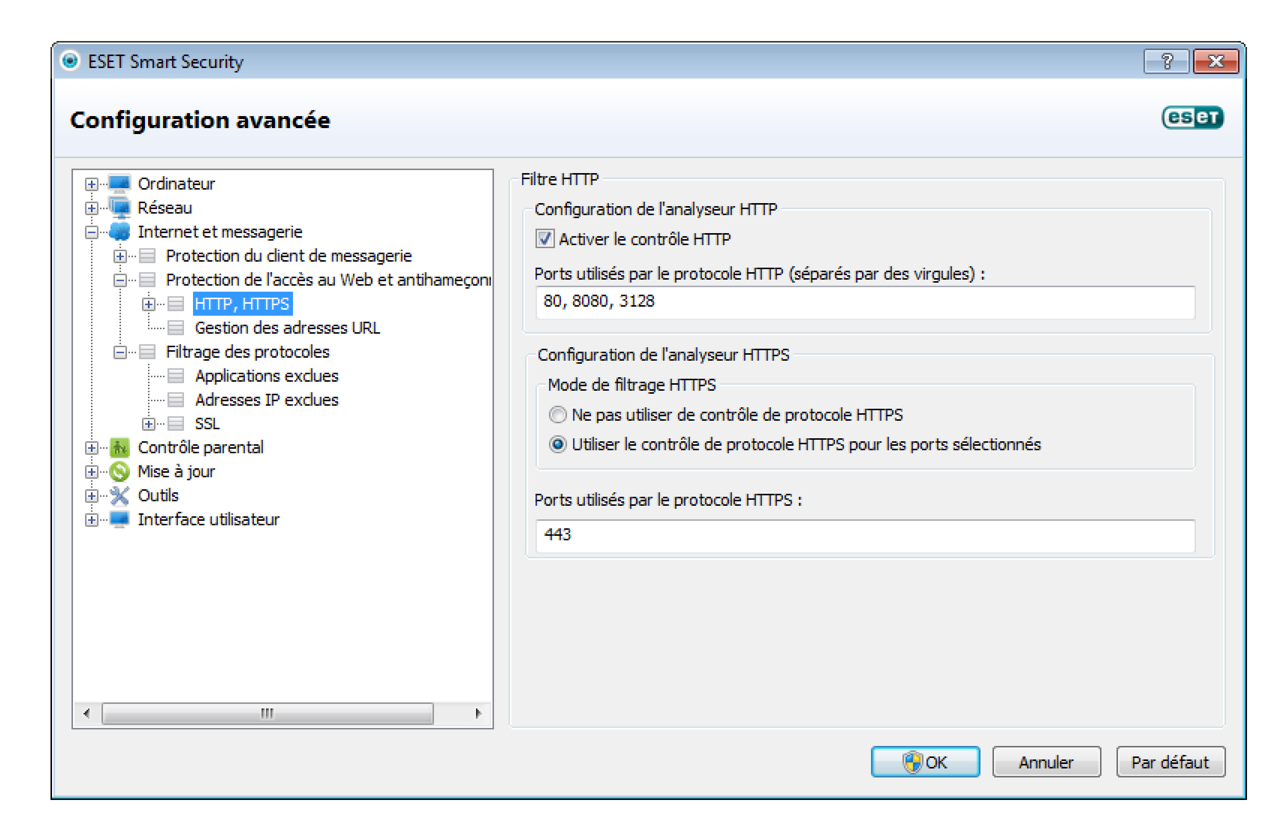
ESET Smart Security prend en charge le contrôle de protocole HTTPS. Les communications HTTPS utilisent un canal chiffré pour transférer des informations entre un serveur et un client. ESET Smart Security contrôle les communications à l'aide des méthodes de chiffrement SSL (Secure Socket Layer) et TLS (Transport Layer Security). Le contrôle HTTPS peut être effectué dans les modes suivants :

Ne pas utiliser de contrôle de protocole HTTPS - Les communications chiffrées ne sont pas vérifiées.

Utiliser le contrôle de protocole HTTPS pour les ports sélectionnés - Le contrôle HTTPS n'a lieu que pour les ports définis dans **Ports utilisés par le protocole HTTPS**.

Utiliser le contrôle de protocole HTTPS pour les ports sélectionnés - Le programme ne contrôle que les applications spécifiées dans la section Navigateurs et qui utilisent les ports définis dans **Ports utilisés par le protocole HTTPS**. Le port 443 est défini par défaut.

La communication chiffrée n'est pas vérifiée. Pour activer l'analyse de la communication chiffrée et afficher la configuration de l'analyseur, accédez à l'option Contrôle de protocole SSL dans la section Configuration avancée, cliquez sur **Internet et messagerie** > **Filtrage des protocoles** > **SSL**, et activez l'option **Toujours analyser le protocole SSL**.



4.3.1.1.1 Mode actif pour les navigateurs Web

ESET Smart Security contient également le sous-menu **Mode actif** qui définit le mode de contrôle des navigateurs Internet.

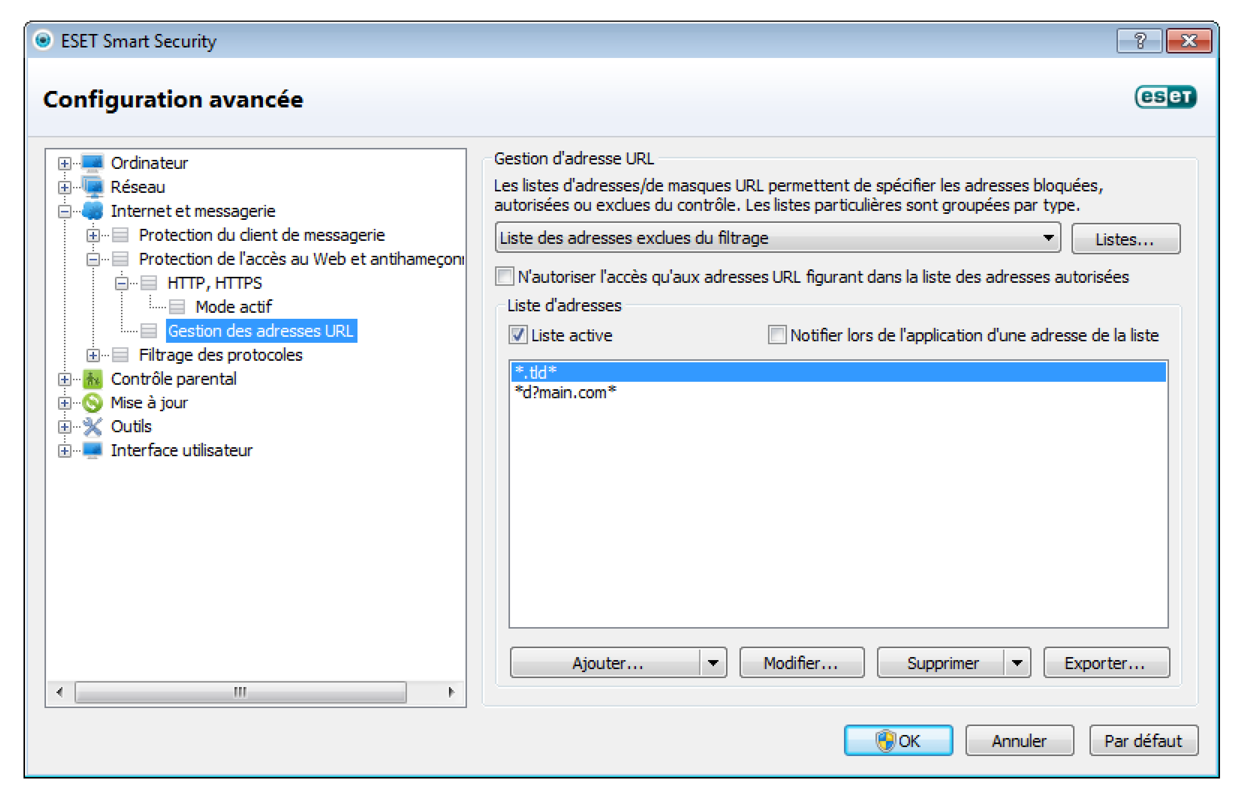
Le **mode actif** est utile, car il examine les données transférées à partir des applications qui accèdent à Internet, qu'elles soient ou non marquées comme navigateurs Web (pour plus d'informations, voir Web et clients de messagerie). Si le Mode actif n'est pas activé, la communication des applications est contrôlée progressivement, par lots. La vérification des données est alors moins efficace, mais la compatibilité avec les applications répertoriées est meilleure. Si le Mode actif ne pose pas de problèmes, nous recommandons de l'activer en cochant la case située à côté de l'application souhaitée. Voici comment fonctionne le mode actif : lorsqu'une application contrôlée télécharge des données, ces dernières sont sauvegardées dans un fichier temporaire créé par ESET Smart Security. Les données ne sont pas encore accessibles par l'application. Une fois le téléchargement terminé, les données sont vérifiées afin de rechercher toute présence de code malveillant. Si aucune infiltration n'est trouvée, les données sont envoyées à l'application. Avec ce processus, les communications réalisées par des applications contrôlées sont intégralement contrôlées. Si le mode passif est activé, les données sont envoyées à l'application par petites quantités pour éviter tout retard.

4.3.1.2 Gestion d'adresse URL

La section Gestion d'adresse URL permet de spécifier des listes d'adresses HTTP qui seront bloquées, autorisées ou exclues de la vérification. Les boutons **Ajouter**, **Modifier**, **Supprimer** et **Exporter** permettent de gérer les listes d'adresses. Les sites Web figurant dans la liste des adresses bloquées ne seront pas accessibles. Les sites Web figurant dans la liste des adresses exclues sont accessibles sans aucune analyse de code malveillant. Si vous sélectionnez l'option **N'autoriser l'accès qu'aux adresses URL figurant dans la liste des adresses autorisées** ; seules les adresses figurant dans la liste des adresses autorisées sont accessibles ; toutes les autres adresses HTTP sont bloquées.

Si vous ajoutez une adresse URL à la **liste des adresses exclues du filtrage**, l'adresse est exclue de l'analyse. Vous pouvez également autoriser ou bloquer certaines adresses en les ajoutant à la **liste des adresses autorisées** ou à la **liste des adresses bloquées**. Lorsque vous cliquez sur le bouton **Listes...**, la fenêtre **Listes d'adresses HTTP/masques** apparaît. Vous pouvez **ajouter** ou **supprimer** des listes d'adresses. Pour ajouter une adresse URL HTTPS à la liste, l'option **Toujours analyser le protocole SSL** doit être active.

Dans toutes les listes, vous pouvez utiliser les symboles spéciaux « * » (astérisque) et « ? » (point d'interrogation). L'astérisque remplace n'importe quelle chaîne de caractères, tandis que le point d'interrogation remplace n'importe quel caractère. Un soin particulier doit être apporté à la spécification des adresses exclues, car la liste ne doit contenir que des adresses sûres et de confiance. De la même manière, veillez à employer correctement les symboles « * » et « ? » dans cette liste. Pour activer une liste, sélectionnez l'option **Liste active**. Pour être informé lors de l'entrée d'une adresse à partir de la liste actuelle, sélectionnez l'option **Notifier lors de l'application d'une adresse de la liste**.



Ajouter.../À partir du fichier - Permet d'ajouter une adresse à la liste, soit manuellement (**Ajouter**), soit à partir d'un simple fichier texte (**À partir du fichier**). L'option **À partir du fichier** permet d'ajouter plusieurs adresses URL/masques qui sont enregistrés dans un fichier texte.

Modifier... - Permet de modifier manuellement des adresses, par exemple en ajoutant un masque (« * » et « ? »).

Supprimer/Supprimer tout - Cliquez sur **Supprimer** pour supprimer l'adresse sélectionnée dans la liste. Pour supprimer toutes les adresses, cliquez sur **Tout supprimer**.

Exporter... - Permet d'enregistrer des adresses de la liste actuelle dans un simple fichier texte.

4.3.2 Protection des clients de messagerie

La protection de la messagerie offre le contrôle de la communication par courrier électronique effectuée via les protocoles POP3 et IMAP. ESET Smart Security utilise le plugin pour Microsoft Outlook et d'autres clients de messagerie pour contrôler toutes les communications impliquant le client de messagerie (POP3, MAPI, IMAP, HTTP). Lorsqu'il examine les messages entrants, le programme utilise toutes les méthodes d'analyse avancées offertes par le moteur d'analyse ThreatSense. Autrement dit, la détection des programmes malveillants s'effectue avant la comparaison avec la base des signatures de virus. L'analyse des communications via le protocole POP3 et IMAP est indépendante du client de messagerie utilisé.

Les options de cette fonctionnalité sont disponibles dans **Configuration avancée** > **Internet et messagerie** > **Protection du client de messagerie**.

Configuration des paramètres du moteur ThreatSense - La configuration avancée de l'analyseur de virus permet de configurer les cibles à analyser, les méthodes de détection, etc. Cliquez sur **Configuration...** pour afficher la fenêtre de configuration détaillée de l'analyseur de virus.

Après la vérification d'un courrier, une notification avec le résultat de l'analyse peut être ajoutée au message. Vous pouvez sélectionner les options **Ajouter une notification aux messages reçus et lus** et **Ajouter une notification aux messages envoyés**. Les notifications ne peuvent pas être transmises sans question, car elles risquent d'être ignorées par les messages HTML problématiques ou même faussées par certains virus. Les notifications peuvent être ajoutées au courrier reçu/lu ou envoyé, ou aux deux. Les options disponibles sont les suivantes :

- **Jamais** - Aucune notification n'est ajoutée.
- **Aux e-mails infectés seulement** - Seuls les messages contenant un code malveillant sont marqués comme contrôlés (valeur par défaut).
- **Aux e-mails infectés seulement** - Le programme ajoute des messages à tout courrier analysé.

Ajouter une note à l'objet des messages infectés reçus et lus/envoyés - Cochez cette case si vous souhaitez que le protection de la messagerie ajoute un avertissement de virus dans l'objet d'un e-mail infecté. Cette fonctionnalité permet tout simplement de filtrer les courriers infectés en fonction de son objet (s'il est pris en charge par le programme

de messagerie). Elle augmente également la crédibilité du destinataire et, en cas de détection d'une infiltration, fournit des informations précieuses sur le niveau de menace d'un message ou d'un expéditeur.

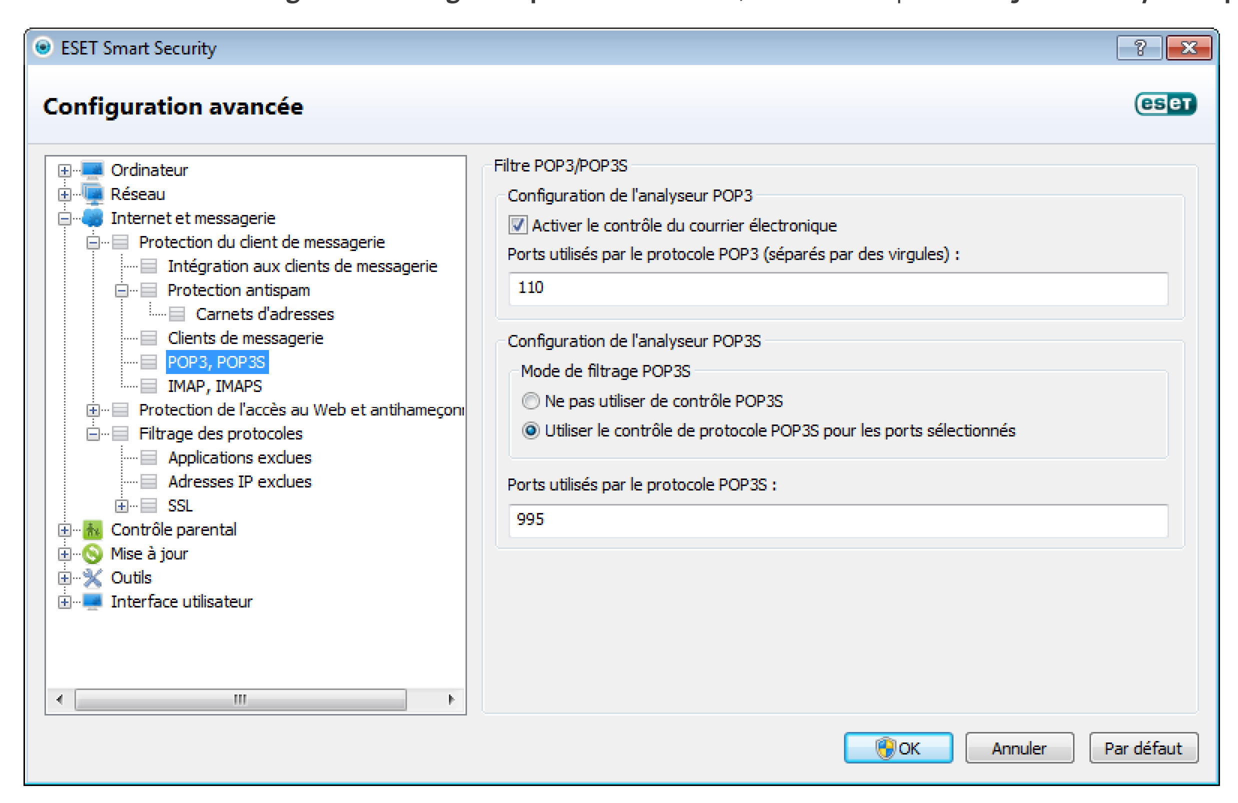
Texte ajouté à l'objet des messages infectés - Modifiez ce texte si vous souhaitez modifier le format du préfixe de l'objet d'un courrier infecté. Cette fonction remplace l'objet du message "*Bonjour*" par le préfixe "*[virus]*" au format suivant : "*[virus] Bonjour*". La variable *%VIRUSNAME%* représente la menace détectée.

4.3.2.1 Filtre POP3, POP3S

Le protocole POP3 est le protocole le plus répandu pour la réception de messages dans un client de messagerie. ESET Smart Security protège ce protocole, quel que soit le client de messagerie utilisé.

Le module de protection qui assure ce contrôle est automatiquement lancé au démarrage du système d'exploitation et reste ensuite actif en mémoire. Pour que le module fonctionne correctement, assurez-vous qu'il est activé. Le contrôle POP3 s'effectue automatiquement sans qu'il faille reconfigurer le client de messagerie. Par défaut, toute communication sur le port 110 est soumise à une analyse, mais d'autres ports de communication peuvent être ajoutés au besoin. Les différents numéros de ports doivent être séparés par une virgule.

La communication chiffrée n'est pas vérifiée. Pour activer l'analyse de la communication chiffrée et afficher la configuration de l'analyseur, accédez à l'option Contrôle de protocole SSL dans la section Configuration avancée, cliquez sur **Internet et messagerie** > **Filtrage des protocoles** > **SSL**, et activez l'option **Toujours analyser le protocole SSL**.



Dans cette section, vous pouvez configurer le contrôle des protocoles POP3 et POP3S.

Activer le contrôle du courrier électronique - Si cette option est activée, les codes malveillants sont recherchés dans tout le trafic POP3.

Ports utilisés par le protocole POP3S - Liste des ports utilisés par le protocole POP3 (110 par défaut).

ESET Smart Security prend également en charge le contrôle du protocole POP3S. Ce type de communication utilise un canal chiffré pour transférer des informations entre un serveur et un client. ESET Smart Security contrôle les communications à l'aide des méthodes de chiffrement SSL (Secure Socket Layer) et TLS (Transport Layer Security).

Ne pas utiliser de contrôle de protocole POP3S - Les communications chiffrées ne sont pas vérifiées.

Utiliser le contrôle de protocole POP3S pour les ports sélectionnés - Activez cette option pour ne permettre le contrôle POP3S que pour les ports définis dans **Ports utilisés par le protocole POP3S**.

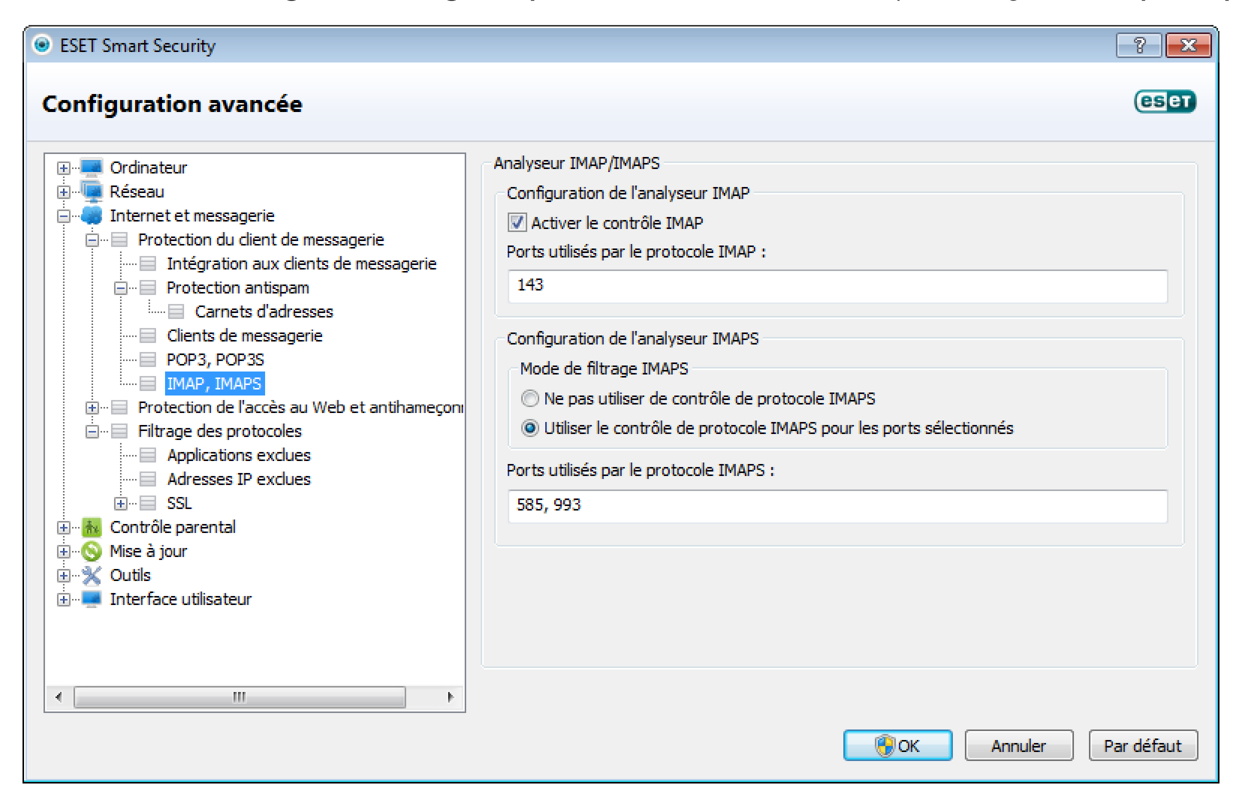
Ports utilisés par le protocole POP3S - Liste des ports POP3S à contrôler (995 par défaut).

4.3.2.2 Contrôle de protocole IMAP, IMAPS

Le protocole IMAP (Internet Message Access Protocol) est un autre protocole Internet qui permet de récupérer les courriers électroniques. Le protocole IMAP présente un certain nombre d'avantages sur le protocole POP3 : par exemple, plusieurs clients peuvent se connecter simultanément à la même boîte aux lettres et tenir à jour les informations sur l'état du message (s'il a été lu, supprimé, ou encore si une réponse a été envoyée). ESET Smart Security fournit une protection pour ce protocole, quel que soit le client de messagerie utilisé.

Le module de protection qui assure ce contrôle est automatiquement lancé au démarrage du système d'exploitation et reste ensuite actif en mémoire. Pour que le module fonctionne correctement, assurez-vous qu'il est activé. Le contrôle IMAP s'effectue automatiquement sans qu'il faille reconfigurer le client de messagerie. Par défaut, toute communication sur le port 143 est soumise à une analyse, mais d'autres ports de communication peuvent être ajoutés au besoin. Les différents numéros de ports doivent être séparés par une virgule.

La communication chiffrée n'est pas vérifiée. Pour activer l'analyse de la communication chiffrée et afficher la configuration de l'analyseur, accédez à l'option Contrôle de protocole SSL dans la section Configuration avancée, cliquez sur **Internet et messagerie** > **Filtrage des protocoles** > **SSL**, et activez l'option **Toujours analyser le protocole SSL**.

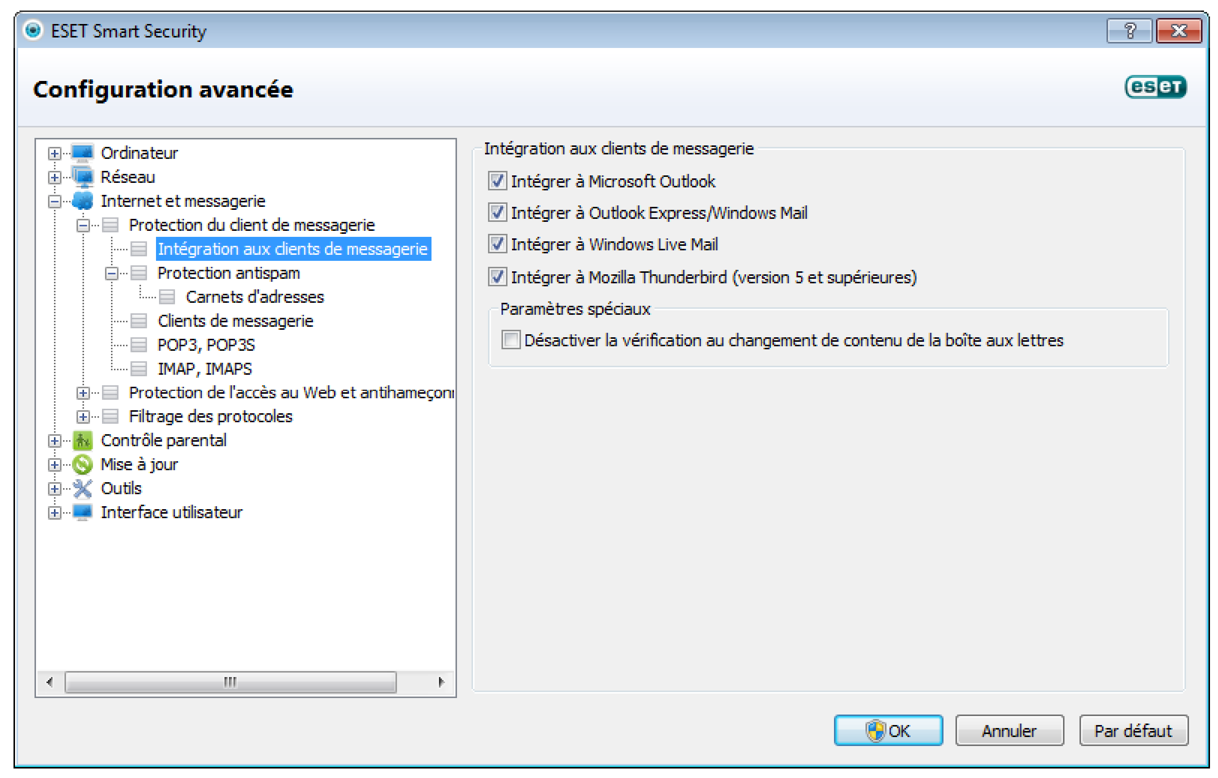


4.3.2.3 Intégration aux clients de messagerie

L'intégration d'ESET Smart Security aux clients de messagerie augmente le niveau de protection active contre les codes malveillants dans les messages électroniques. Si votre client de messagerie est pris en charge, cette intégration peut être activée dans ESET Smart Security. Si l'intégration est activée, la barre d'outils ESET Smart Security est insérée directement dans le client de messagerie, ce qui permet de protéger les messages plus efficacement. Les paramètres d'intégration se trouvent dans la section **Configuration** > **Accéder à la configuration avancée...** > **Internet et messagerie** > **Protection du client de messagerie** > **Intégration aux clients de messagerie**.

Les clients de messagerie pris en charge sont Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail et Mozilla Thunderbird. Pour obtenir une liste complète des clients de messagerie pris en charge, avec leur version, reportez-vous à cet article de la base de connaissances ESET.

Sélectionnez l'option **Désactiver la vérification au changement de contenu de la boîte aux lettres** si vous constatez un ralentissement du système lors de l'utilisation du client de messagerie. Une telle situation peut se présenter lors du téléchargement de messages à partir du magasin Kerio Outlook Connector.



Même si l'intégration n'est pas activée, les communications par messagerie demeurent protégées par le module de protection du client de messagerie (POP3, IMAP).

4.3.2.3.1 Configuration de la protection du client de messagerie

Le module de protection de la messagerie électronique prend en charge les clients de messagerie suivants : Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail et Mozilla Thunderbird. Ce module fonctionne comme un module plugin pour ces programmes. L'avantage principal du contrôle par plugin réside dans le fait qu'il est indépendant du protocole utilisé. Lorsqu'un client de messagerie reçoit un message chiffré, il le déchiffre et l'envoie à l'analyseur de virus.

Courriers électroniques à analyser

Courrier reçu - Active/désactive la vérification des messages reçus.
Courrier envoyé - Active/désactive la vérification des messages envoyés.
Courrier lu - Active/désactive la vérification des messages lus.

Action à effectuer sur les courriers électroniques infectés

Aucune action - Si cette option est activée, le programme identifie les pièces jointes infectées, mais n'entreprend aucune action sur les messages concernés.
Supprimer les courriers - Le programme avertit l'utilisateur à propos de l'infiltration ou des infiltrations et supprime le message.
Déplacer les courriers vers le dossier Éléments supprimés - Les courriers infectés sont automatiquement placés dans le dossier **Éléments supprimés**.
Déplacer les courriers vers le dossier - Spécifiez le dossier personnalisé dans lequel les courriers infectés doivent être déplacés lors de leur détection.

Autre

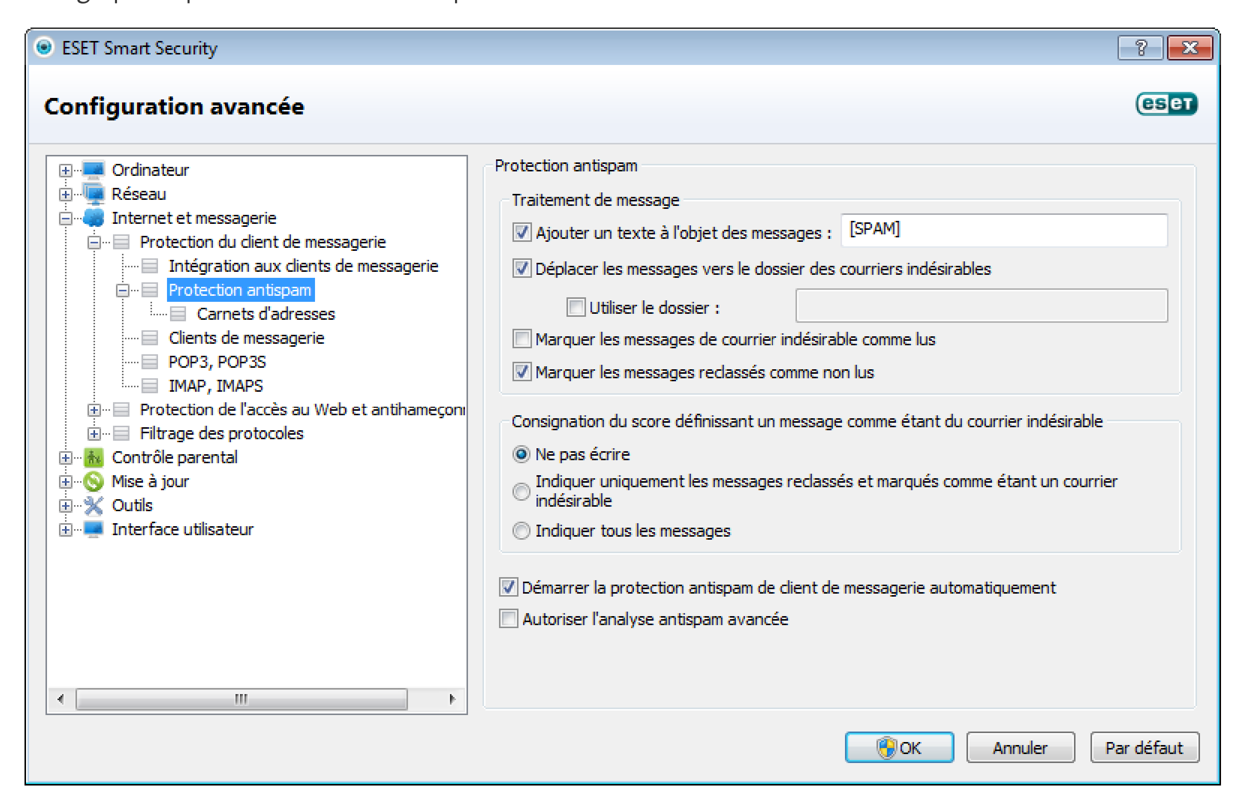
Répéter l'analyse après mise à jour - Active/désactive la répétition de l'analyse après la mise à jour de la base des signatures de virus.
Accepter les résultats d'analyse d'autres modules - Si cette option est activée, le module de protection de messages accepte les résultats d'analyse d'autres modules de protection.

4.3.2.4 Suppression d'infiltrations

En cas de réception d'un message infecté, une fenêtre d'alerte s'affiche. Cette fenêtre indique le nom de l'expéditeur, son message et le nom de l'infiltration. La partie inférieure de la fenêtre présente les options disponibles concernant l'objet détecté : **Nettoyer**, **Supprimer** ou **Aucune action**. Dans la plupart des cas, nous recommandons de sélectionner **Nettoyer** ou **Supprimer**. Dans les situations particulières où vous souhaitez vraiment recevoir le fichier infecté, sélectionnez **Aucune action**. Si le niveau **Nettoyage strict** est activé, une fenêtre d'information sans options s'affiche.

4.3.3 Protection antispam

Le courrier non sollicité, ou spam, constitue l'un des plus grands problèmes liés à la communication électronique. Le spam représente jusqu'à 80 % de toutes les communications par messagerie électronique. La protection antispam sert à vous prémunir de ce problème. En combinant plusieurs principes efficaces, le module antispam garantit un meilleur filtrage pour que votre boîte de réception reste saine.



La détection de spam reconnaît le courrier non sollicité d'après des listes prédéfinies d'adresses fiables (liste blanche) et de spam (liste noire). Toutes les adresses de votre liste de contacts sont automatiquement ajoutées à la liste blanche, ainsi que toutes les autres adresses que vous désignez comme sûres.

La principale méthode utilisée pour détecter du courrier indésirable est l'analyse des propriétés des messages. Les messages reçus sont analysés selon des critères antispam de base (définitions de messages, heuristique statistique, algorithmes de reconnaissance et autres méthodes uniques). L'indice qui en résulte détermine si un message est du spam ou non.

La protection antispam dans ESET Smart Security vous permet de définir différents paramètres à utiliser avec les listes de messagerie. Les options sont les suivantes :

Démarrer la protection antispam de client de messagerie automatiquement - Active/désactive la protection antispam du client de messagerie.

Traitement des messages

Ajouter un texte à l'objet des messages - Permet d'ajouter une chaîne de caractères personnalisée à la ligne de l'objet des messages classés comme courrier indésirable. La valeur par défaut est [SPAM].

Déplacer les messages vers le dossier des courriers indésirables - Lorsque cette option est sélectionnée, les messages de courrier indésirable sont déplacés vers le dossier de courrier indésirable par défaut.

Utiliser le dossier - Cette option permet le déplacement des messages spam vers un dossier défini par l'utilisateur.

Marquer les messages de courrier indésirable comme lus - Sélectionnez cette option pour marquer automatiquement le courrier indésirable comme lu. Vous pouvez ainsi vous concentrer sur les messages « propres ».

Marquer les messages reclassés comme non lus - Les messages classés au départ comme courrier indésirable, mais marqués ultérieurement comme « propres », sont affichés comme non lus.

Consignation du score définissant un message comme étant du courrier indésirable

Le moteur du blocage de courrier indésirable ESET Smart Security attribue à chaque message analysé un score de courrier indésirable. Le message est enregistré dans le journal du courrier indésirable (**ESET Smart Security** > **Outils** > **Fichiers journaux** > **Protection antispam**).

- **Ne pas écrire** - La cellule **Score** du journal de protection antispam est vide.
- **Indiquer uniquement les messages reclassés et marqués comme étant un courrier indésirable** - Utilisez cette option si vous souhaitez enregistrer un score de courrier indésirable pour les messages marqués comme étant du courrier indésirable.
- **Indiquer tous les messages** - Tous les messages sont enregistrés dans le journal avec un score de courrier indésirable.

Démarrer la protection antispam de client de messagerie automatiquement - Lorsque cette option est activée, la protection antispam est automatiquement activée au démarrage du système.

Activer le contrôle avancé de l'antispam - Des bases de données antispam supplémentaires seront téléchargées, augmentant ainsi les possibilités antispam et produisant de meilleurs résultats.

ESET Smart Security prend en charge la protection antispam pour Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail et Mozilla Thunderbird.

4.3.3.1 Ajout d'adresses à la liste blanche et à la liste noire

Les adresses de messagerie des personnes avec lesquelles vous communiquez régulièrement peuvent être ajoutées à la liste blanche. Ainsi, les messages provenant d'adresses figurant dans la liste blanche ne sont jamais classés comme courrier indésirable. Les adresses connues pour envoyer du courrier indésirable peuvent être ajoutées à la liste noire et sont toujours classées comme émettant du courrier indésirable. Pour ajouter une adresse à la liste blanche ou à la liste noire, cliquez avec le bouton droit sur le courrier électronique et sélectionnez **ESET Smart Security** > **Ajouter à la liste blanche** ou **Ajouter à la liste noire**, ou cliquez sur le bouton **Adresse fiable** ou **Adresse de courrier indésirable** dans la barre d'outils Antispam ESET Smart Security du programme de messagerie.

De la même manière, ce processus s'applique également aux adresses émettant du courrier indésirable. Si une adresse figure dans la liste noire, tous les messages provenant de cette adresse sont classifiés comme du spam.

4.3.3.2 Marquage de messages comme courrier indésirable

Tout message affiché dans votre client de messagerie peut être marqué comme du courrier indésirable. Pour ce faire, cliquez avec le bouton droit sur le message et cliquez sur **ESET Smart Security** > **Reclassifier les messages sélectionnés comme courrier indésirable** ou sur **Adresse de courrier indésirable** dans la barre d'outils Antispam ESET Smart Security située dans la partie supérieure du client de messagerie.

Les messages reclassés sont automatiquement déplacés vers le dossier COURRIER INDÉSIRABLE, mais l'adresse de l'expéditeur n'est pas ajoutée à la liste noire. De même, les messages peuvent être marqués comme « non-spam ». Si des messages du dossier « **Junk E-mail** » sont classés comme non-spam, ils sont déplacés vers leur dossier d'origine. Lorsqu'un message est marqué comme non-courrier indésirable, l'adresse de l'expéditeur n'est pas automatiquement ajoutée à la liste blanche.

4.3.4 Filtrage des protocoles

La protection antivirus des protocoles d'application est fournie par le moteur d'analyse ThreatSense qui intègre en toute transparence toutes les techniques avancées d'analyse des logiciels malveillants. Le contrôle fonctionne automatiquement, indépendamment du navigateur Internet ou du client de messagerie utilisés. Pour les communications chiffrées (SSL), voir **Filtrage des protocoles** > **SSL**.

Activer le filtrage du contenu des protocoles d'application - Si cette option est activée, tout le trafic HTTP(S), POP3(S) et IMAP(S) est contrôlé par l'analyseur antivirus.

REMARQUE : depuis Windows Vista Service Pack 1 et Windows 7, la nouvelle architecture de plateforme de filtrage Windows permet de vérifier les communications réseau. Étant donné que la technologie WFP utilise des techniques de surveillance spéciales, les options suivantes sont indisponibles :

- **Ports HTTP et POP3** - Limite le routage du trafic vers le serveur proxy interne uniquement pour les ports HTTP et POP3.
- **Applications marquées comme navigateurs Internet et clients de messagerie** - Limite le routage du trafic vers le serveur proxy interne uniquement pour les applications marquées comme navigateurs Internet et clients de messagerie. (**Internet et messagerie** > **Filtrage des protocoles** > **Web et clients de messagerie**).
- **Ports et applications marqués comme navigateurs Web ou clients de messagerie** - Active tout le trafic des ports HTTP et POP3, ainsi que toutes les communications des applications marquées comme navigateurs Internet et clients de messagerie vers le serveur proxy interne.

4.3.4.1 Web et clients de messagerie

REMARQUE : depuis Windows Vista Service Pack 1 et Windows 7, la nouvelle architecture de plateforme de filtrage Windows permet de vérifier les communications réseau. Étant donné que la technologie WFP utilise des techniques de surveillance spéciales, la section **Web et clients de messagerie** est indisponible.

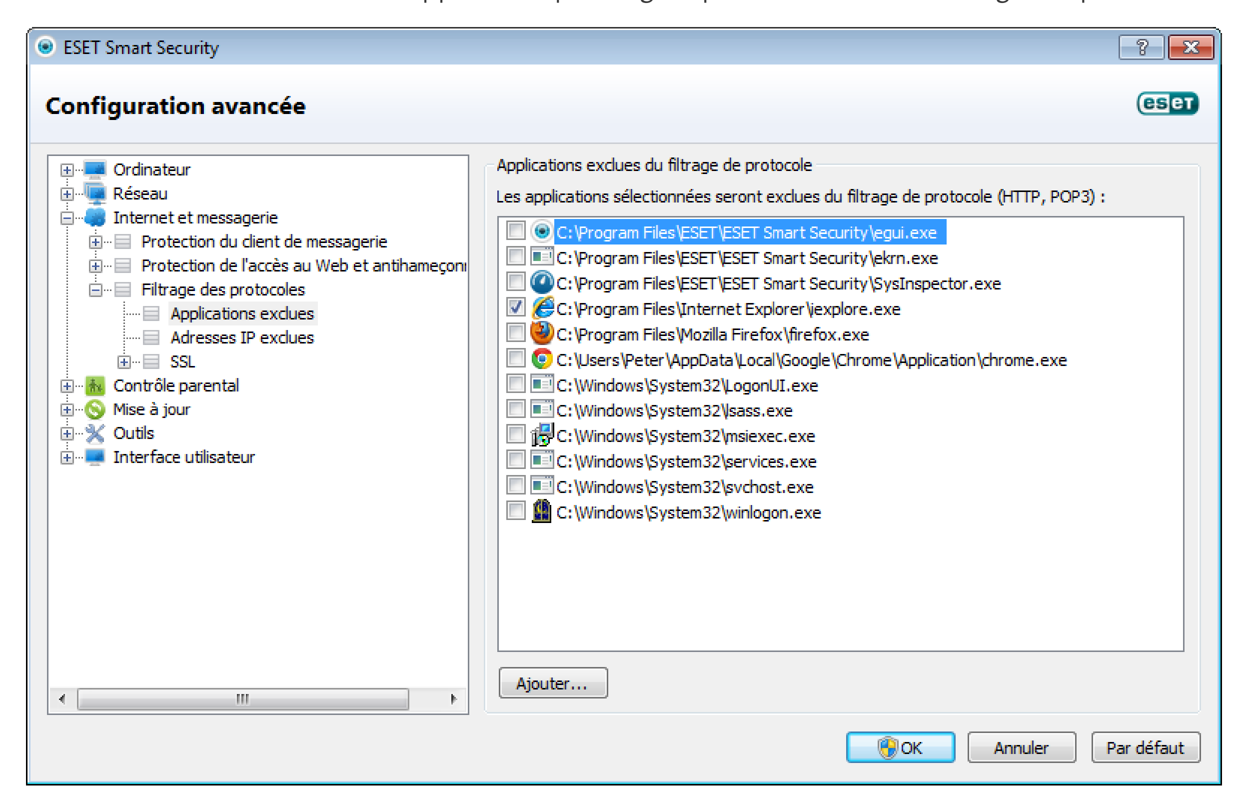
À cause du nombre considérable de codes malveillants circulant sur Internet, la sécurisation de la navigation sur Internet est un aspect très important de la protection des ordinateurs. Les vulnérabilités des navigateurs Internet et les liens frauduleux contribuent à faciliter l'accès imperceptible au système par des codes malveillants. C'est pourquoi ESET Smart Security se concentre sur la sécurité des navigateurs Internet. Chaque application accédant au réseau peut être marquée comme étant un navigateur Internet. La case à cocher a deux états possibles :

- **Non cochée** - La communication des applications est filtrée uniquement pour les ports spéficiés.
- **Cochée** - La communication est toujours filtrée (même si un autre port est défini).

4.3.4.2 Applications exclues

Pour exclure du filtrage de contenu la communication de certaines applications sensibles au réseau, sélectionnez ces applications dans la liste. Les communications HTTP/POP3/IMAP liées aux adresses sélectionnées ne font pas l'objet d'une détection des menaces. Il est recommandé d'utiliser cette option uniquement pour les applications qui ne fonctionnent pas correctement lorsque leur communication est vérifiée.

L'exécution des applications et des services est disponible automatiquement. Cliquez sur le bouton **Ajouter...** pour sélectionner manuellement une application qui ne figure pas dans la liste des filtrages de protocole.

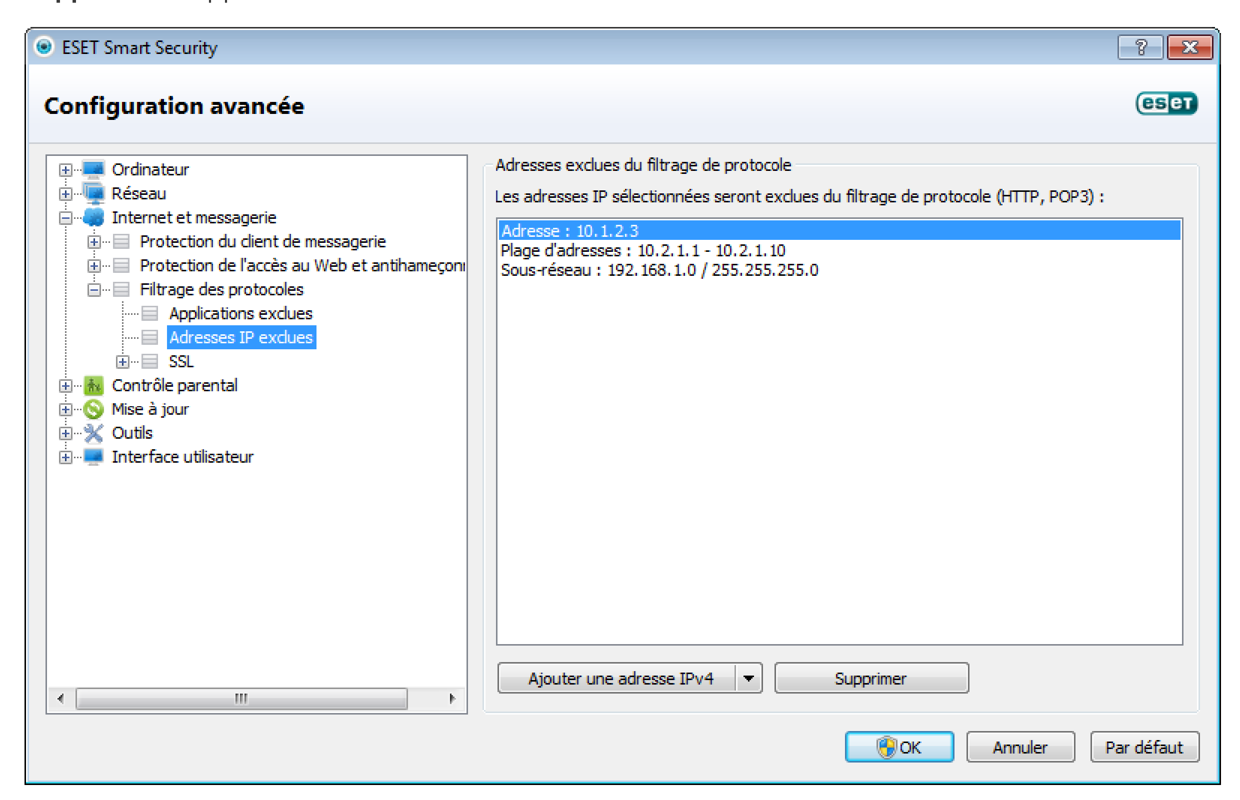


4.3.4.3 Adresses IP exclues

Les adresses figurant dans cette liste sont exclues du filtrage du contenu des protocoles. Les communications HTTP/POP3/IMAP liées aux adresses sélectionnées ne font pas l'objet d'une détection des menaces. Il est recommandé d'utiliser cette option uniquement pour les adresses fiables.

Ajouter une adresse IPv4/IPv6 - Cette option permet d'ajouter une adresse/une plage d'adresses/un sous-réseau IP d'un point distant auquel la règle doit être appliquée.

Supprimer - Supprime les entrées sélectionnées de la liste.



4.3.4.3.1 Ajouter une adresse IPv4

Cette option permet d'ajouter une adresse IP/une plage d'adresses/un sous-réseau d'un point distant pour lequel la règle est appliquée. Le protocole Internet version 4 est l'ancienne version, mais il est toujours largement utilisé.

Adresse unique - Ajoute l'adresse IP d'un ordinateur auquel appliquer la règle (par exemple *192.168.0.10*)

Plage d'adresses - Saisissez l'adresse IP de début et de fin pour définir la plage IP (de plusieurs ordinateurs) à laquelle la règle doit être appliquée (par exemple *192.168.0.1* à *192.168.0.99*).

Sous-réseau - Le sous-réseau (groupe d'ordinateurs) est défini par une adresse IP et un masque.

Par exemple, *255.255.255.0* est le masque réseau du préfixe *192.168.1.0/24*, ce qui signifie que la plage d'adresses est comprise entre *192.168.1.1* à *192.168.1.254*.

4.3.4.3.2 Ajouter une adresse IPv6

Cette option permet d'ajouter une adresse IPv6/un sous-réseau d'un point distant pour lequel la règle est appliquée. Il s'agit de la version la plus récente du protocole Internet et elle remplacera la version 4 plus ancienne.

Adresse unique - Ajoute l'adresse IP d'un ordinateur auquel la règle doit être appliquée, par exemple *2001:718:1c01:16:214:22ff:fec9:ca5*.

Sous-réseau - Le sous-réseau (groupe d'ordinateurs) est défini par une adresse IP et un masque (par exemple : *2002:c0a8:6301:1::1/64*).

4.3.4.4 Contrôle de protocole SSL

ESET Smart Security vous permet de vérifier les protocoles encapsulés dans le protocole SSL. Vous pouvez utiliser plusieurs modes d'analyse pour les communications SSL protégées à l'aide de certificats approuvés, de certificats inconnus ou de certificats exclus de la vérification des communications SSL protégées.

Toujours analyser le protocole SSL - Sélectionnez cette option pour analyser toutes les communications SSL protégées, à l'exception des communications protégées par des certificats exclus de la vérification. Si une nouvelle communication utilisant un certificat signé inconnu est établie, vous n'êtes pas informé et la communication est automatiquement filtrée. Lorsque vous accédez à un serveur disposant d'un certificat non approuvé et que vous marquez comme étant approuvé (il est ajouté à la liste des certificats approuvés), la communication vers le serveur est autorisée et le contenu du canal de communication est filtré.

Demander pour les sites non visités (des exclusions peuvent être définies) - Si vous accédez à un nouveau site protégé par SSL (dont le certificat est inconnu), vous êtes invité à confirmer que vous souhaitez le visiter avant d'être autorisé à le faire. Ce mode vous permet de créer la liste des certificats SSL qui seront exclus de l'analyse.

Ne pas analyser le protocole SSL - Si cette option est activée, le programme n'analyse pas les communications SSL.

Appliquer les exceptions créées sur la base de certificats - Active l'utilisation d'exclusions spécifiées dans les certificats exclus et fiables pour l'analyse de la communication SSL. Cette option est disponible si vous sélectionnez **Toujours analyser le protocole SSL**.

Bloquer les communications chiffrées à l'aide du protocole obsolète SSL v2 - Les communications utilisant la version antérieure du protocole SSL sont automatiquement bloquées.

4.3.4.4.1 Certificats

Pour que la communication SSL fonctionne correctement dans les navigateurs/clients de messagerie, il est essentiel d'ajouter le certificat racine pour ESET, spol s r.o. à la liste des certificats racines connus (éditeurs). Par conséquent, l'option **Ajouter le certificat racine aux navigateurs connus** doit être activée. Activez cette option pour ajouter manuellement le certificat racine d'ESET aux navigateurs connus (Opera, Firefox par exemple). Pour les navigateurs utilisant le magasin de certification système (Internet Explorer par exemple), le certificat est ajouté automatiquement. Pour appliquer le certificat à des navigateurs non pris en charge, cliquez sur **Afficher le certificat** > **Détails** > **Copier dans un fichier...**, puis importez-le manuellement dans le navigateur.

Dans certains cas, il est impossible de vérifier le certificat à l'aide du magasin d'Autorités de certification racine de confiance (VeriSign par exemple). Cela signifie que le certificat est signé automatiquement par un utilisateur (l'administrateur d'un server Web ou une petite entreprise) et que le fait de le considérer comme fiable n'est pas toujours un risque. La plupart des grandes entreprises (les banques par exemple) utilisent un certificat signé par TRCA. Si l'option **Interroger sur la validité du certificat** est activée (par défaut), l'utilisateur est invité à sélectionner une action à entreprendre lorsque la communication chiffrée est établie. Une boîte de dialogue de sélection d'action apparaît ; vous pouvez décider de marquer le certificat comme étant fiable ou exclu. Si le certificat ne figure pas dans la liste TRCA, la fenêtre est rouge. S'il y figure, la fenêtre est verte.

Vous pouvez sélectionner l'option **Bloquer toute communication utilisant le certificat** pour toujours mettre fin à la connexion chiffrée au site utilisant le certificat non vérifié.

Si le certificat n'est pas valide ou est endommagé, cela signifie qu'il est arrivé à expiration ou que sa signature automatique est incorrecte. Dans ce cas, il est recommandé de bloquer la communication qui utilise le certificat.

4.3.4.4.1.1 Certificats approuvés

Outre le magasin TRCA intégré dans lequel ESET Smart Security stocke les certificats approuvés, vous pouvez créer une liste personnalisée de certificats approuvés qui est accessible dans **Configuration avancée** (F5) > **Internet et messagerie** > **Filtrage des protocoles** > **SSL** > **Certificats** > **Certificats approuvés**. ESET Smart Security vérifie le contenu des communications chiffrées qui utilisent les certificats figurant dans cette liste.

Pour supprimer des éléments sélectionnés dans la liste, cliquez sur le bouton **Supprimer**. Cliquez sur l'option **Afficher** (ou double-cliquez sur le certificat) pour afficher les informations concernant le certificat sélectionné.

4.3.4.4.1.2 Certificats exclus

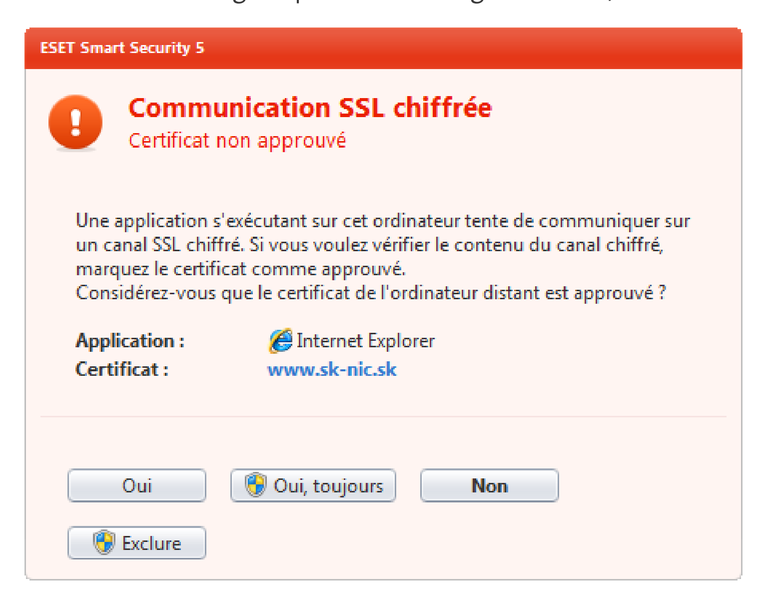
La section Certificats exclus contient des certificats considérés comme étant sûrs. Le contenu des communications chiffrées qui utilisent les certificats répertoriés dans la liste des certificats exclus ne fait pas l'objet de recherche de menaces. Il est recommandé de n'exclure que les certificats Web qui sont garantis comme étant sécurisés et dont la communication utilisant les certificats n'a pas besoin d'être vérifiée. Pour supprimer des éléments sélectionnés dans la liste, cliquez sur le bouton **Supprimer**. Cliquez sur l'option **Afficher** (ou double-cliquez sur le certificat) pour afficher les informations concernant le certificat sélectionné.

4.3.4.4.1.3 Communication SSL chiffrée

Si l'ordinateur est configuré pour l'analyse du protocole SSL, la boîte de dialogue vous invitant à choisir une action peut s'afficher en cas de tentative d'établissement d'une communication chiffrée (à l'aide d'un certificat inconnu). La boîte de dialogue contient les informations suivantes : nom de l'application à l'origine de la communication et nom du certificat utilisé.



Si le certificat ne figure pas dans le magasin TRCA, il est considéré comme non fiable.



Les actions suivantes sont disponibles pour les certificats :

Oui - Le certificat est temporairement marqué comme fiable pour la session en cours ; la fenêtre d'alerte ne s'affiche pas à la tentative suivante d'utilisation du certificat.

Oui, toujours - Marque le certificat comme approuvé et l'ajoute à la liste des certificats approuvés ; aucune fenêtre d'alerte ne s'affiche pour les certificats approuvés.

Non - Marque le certificat comme étant non fiable pour la session en cours ; la fenêtre d'alerte s'affiche lors de la tentative suivante d'utilisation du certificat.

Exclure - Ajoute le certificat à la liste des certificats exclus ; les données transférées sur le canal chiffré indiqué ne sont pas du tout vérifiées.

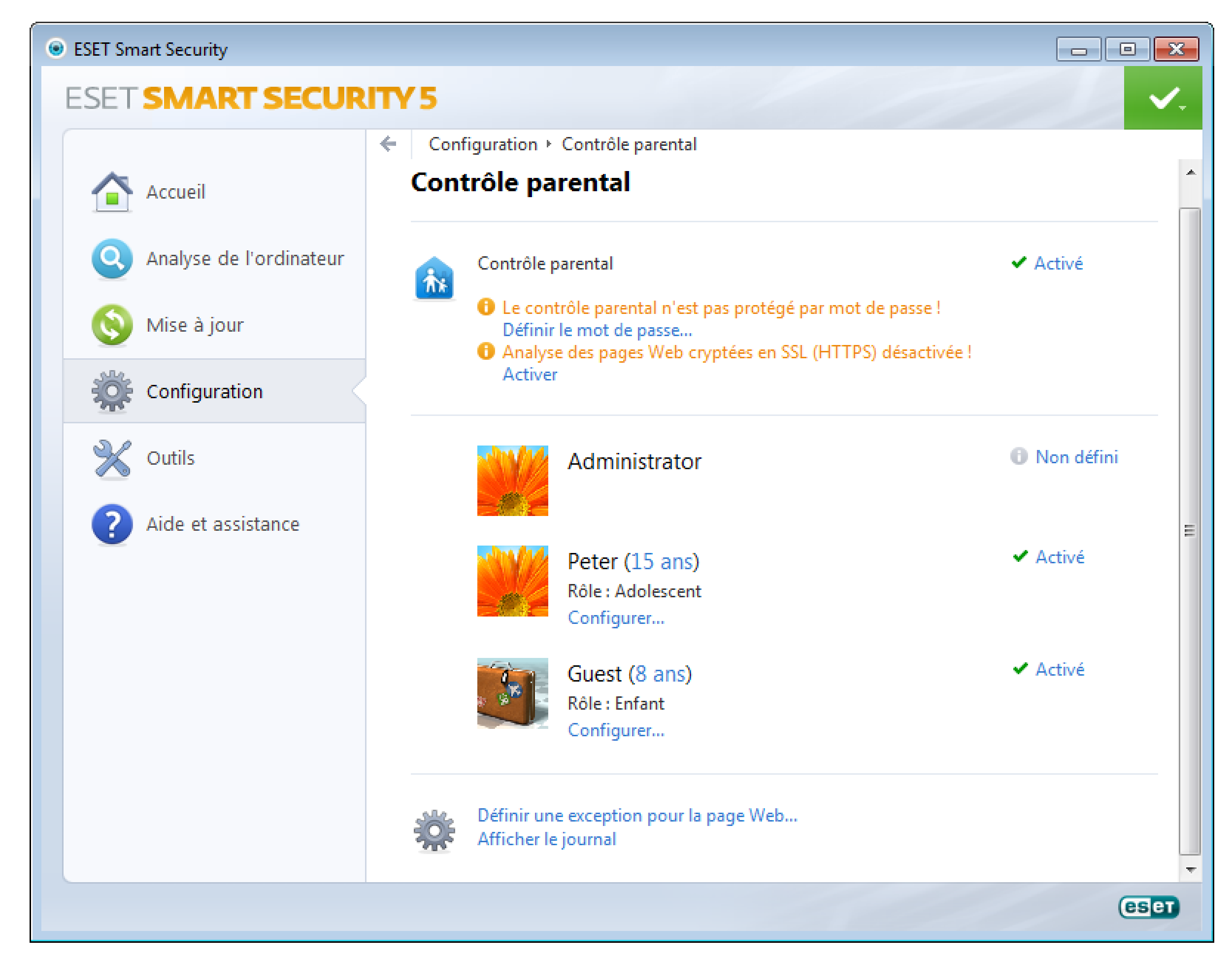
4.4 Contrôle parental

Le module Contrôle parental permet de configurer les paramètres de contrôle parental. Ce système fournit aux parents des outils automatisés qui protègent les enfants et définissent des restrictions d'utilisation des périphériques et des services. L'objectif est d'empêcher les enfants et les jeunes adultes d'accéder à des pages au contenu inapproprié ou nuisible.

Contrôle parental permet de bloquer les pages Web dont le contenu peut être choquant. En outre, les parents, peuvent interdire l'accès à plus de 20 catégories de sites Web prédéfinies et à plus de 140 sous-catégories.

Pour activer le contrôle parental pour un compte utilisateur spécifié, procédez comme suit :

1. Lorsque le Contrôle parental est désactivé dans ESET Smart Security, deux méthodes permettent d'activer le contrôle parental pour un compte utilisateur spécifié :
   - Cliquez sur **Désactivé** dans le volet **Configuration** de la fenêtre principale du programme et remplacez l'état du contrôle parental sur **Activé**.
   - Appuyez sur F5 pour accéder à l'arborescence de **Configuration avancée**, sélectionnez **Contrôle parental**, puis activez la case à côté de **Activer le contrôle parental**.
2. Cliquez sur **Configuration** > **Contrôle parental** dans la fenêtre principale du programme. Même si **Activé** s'affiche en regard de **Contrôle parental**, vous devez configurer le contrôle parental pour le compte souhaité en cliquant sur **Non défini**. Dans la fenêtre Configuration de compte, entrez un âge, afin de déterminer le niveau d'accès et les pages Web adaptées à l'âge qui sont recommandées. Le contrôle parental est désormais activé pour le compte spécifié. Cliquez sur **Configuration** sous un nom de compte pour personnaliser les catégories que vous souhaitez autoriser ou bloquer dans l'onglet Filtrage de contenu des pages Web. Pour autoriser ou bloquer des pages Web personnalisées qui ne correspondent à aucune catégorie, cliquez sur l'onglet Pages Web bloquées et autorisées.



Si vous cliquez sur **Contrôle parental** dans le volet **Configuration** de la fenêtre principale de ESET Smart Security, vous verrez que celle-ci se divise en trois sections.

1. Contrôle parental

Après avoir désélectionné **Activé** sur la droite, la fenêtre **Désactiver temporairement la protection** apparaît. Vous pouvez y définir la durée après laquelle cette protection sera désactivée. L'option devient alors **Désactivé** et tous les paramètres suivants sont masqués.

Il est important de protéger les paramètres ESET Smart Security à l'aide d'un mot de passe. Ce mot de passe peut être défini dans la section Configuration de l'accès. Si aucun mot de passe n'est défini, un avertissement sous l'option **Contrôle parental** - Le *contrôle parental n'est pas protégé par mot de passe !* - et **Définir le mot de passe...** est visible. Les restrictions définies dans le contrôle parental n'ont une incidence que sur les comptes utilisateur standard. L'administrateur pouvant ignorer les restrictions, ces dernières seraient inopérantes.

Les communications HTTPS (SSL) ne sont pas filtrées par défaut. Par conséquent, le contrôle parental ne peut pas bloquer les pages Web qui commencent par *https://*. Pour activer cette fonction, sélectionnez **Activer** en regard du message d'avertissement Analyse des pages Web cryptées en SSL (HTTPS) désactivée ! ou sélectionnez **Toujours analyser le protocole SSL** dans la section **Configuration avancée** > **Internet et messagerie** > **Filtrage de protocoles** > **SSL**.

Remarque : Le contrôle parental nécessite que les options Filtrage du contenu des protocoles d'application, Contrôle du protocole HTTPS et Intégration système du pare-feu personnel soient activées pour fonctionner correctement. Toutes ces fonctionnalités sont activées par défaut.

2. Comptes utilisateur Windows

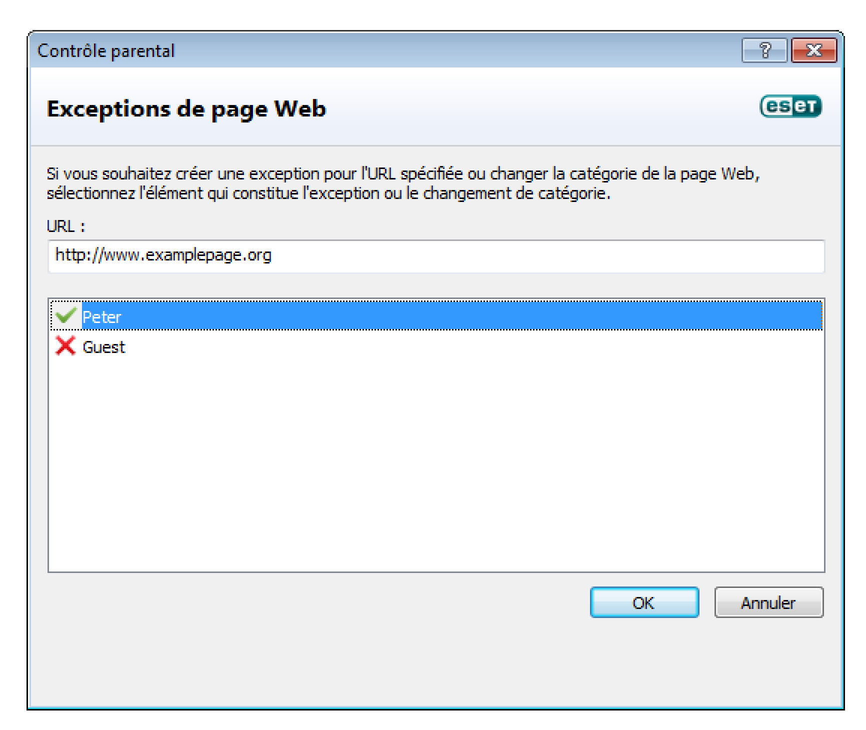
Si vous avez créé un rôle pour un compte existant, il s'affichera ici avec l'attribut **Activé**. Le fait de cliquer sur l'option **Activé** désactive le contrôle parental pour le compte. Sous un compte actif, cliquez sur **Configuration...** pour voir la liste des catégories autorisées de pages Web de ce compte ainsi que les pages Web bloquées et autorisées.

Important : pour créer un nouveau compte (par exemple, pour un enfant), utilisez les instructions ci-après pour Windows 7 ou Windows Vista :

1. Ouvrez **Comptes utilisateur** en cliquant sur le bouton **Démarrer** (situé en bas à gauche sur le Bureau), sur **Panneau de configuration**, puis sur **Comptes utilisateur**.
2. Cliquez sur **Gérer un autre compte**. Si vous y êtes invité, saisissez le mot de passe de l'administrateur ou confirmez.
3. Cliquez sur **Créer un compte**.
4. Saisissez le nom que vous souhaitez donner au compte, cliquez sur un type de compte, puis sur **Créer un compte**.
5. Dans la fenêtre principale du programme ESET Smart Security, cliquez à nouveau sur **Configuration** > **Contrôle parental** pour rouvrir le volet de contrôle parental.

3. La dernière section contient deux options

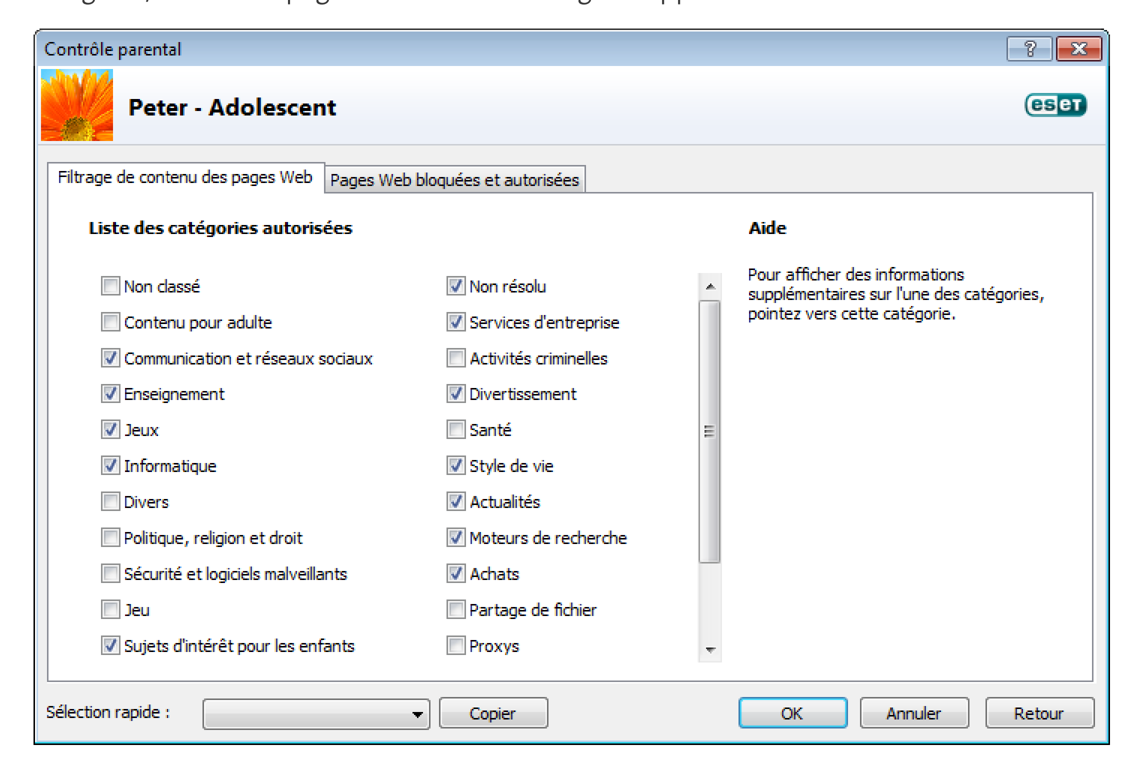
Définir une exception pour la page Web... - Cette méthode permet de définir rapidement une exception concernant une page Web pour le compte sélectionné. Entrez l'adresse URL de la page Web dans le champ **URL** et sélectionnez le compte dans la liste au-dessous. Si vous sélectionnez la case **Bloquer**, la page Web est bloquée pour ce compte. Si vous ne cochez pas cette case, la page Web est autorisée. Les exceptions définies ici sont prioritaires sur les catégories définies pour le ou les comptes sélectionnés. Par exemple, si la catégorie **Actualités** est bloquée pour un compte, mais que vous avez défini une page Web d'actualités en tant qu'exception, le compte peut accéder à cette page. Vous pouvez consulter les modifications apportées ici dans la section Pages Web bloquées et autorisées.



Afficher les fichiers journaux - Cette option affiche le journal détaillé de l'activité de contrôle parental (pages bloquées, compte pour lequel la page est bloquée, motif, etc.). Vous pouvez également filtrer ce journal en fonction des critères de votre choix en cliquant sur **Filtrer...**.

4.4.1 Liste des catégories de pages Web autorisées

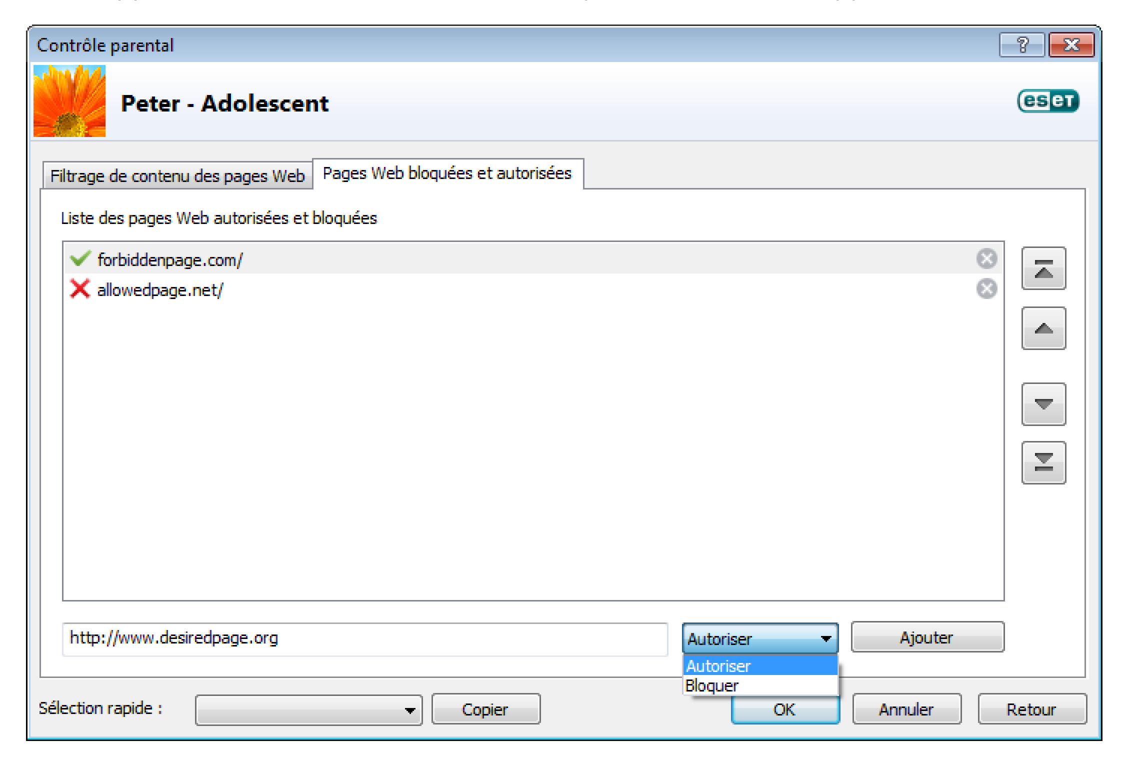
Si la case en regard d'une catégorie est cochée, cela signifie que la catégorie est autorisée. Pour bloquer une catégorie pour le compte sélectionné, vous devez désactiver cette case. Si vous immobilisez le pointeur de la souris sur une catégorie, la liste des pages Web de cette catégorie apparaît.



L'option **Sélection rapide** permet de sélectionner un profil prédéfini (**Enfant**, **Parent** et **Adolescent**) ou un compte créé par l'utilisateur, puis de cliquer sur **Copier** pour copier la **liste des catégories autorisées** depuis ces comptes.

4.4.2 Pages Web bloquées et autorisées

La liste des pages Web autorisées se trouve à gauche et la liste des pages Web bloquées à droite. Entrez une adresse URL dans le champ vide sous la liste, sélectionnez **Autoriser** ou **Bloquer** et cliquez sur **Ajouter** pour l'ajouter à la liste. Pour supprimer une adresse URL de la liste, cliquez sur le bouton Supprimer .



Dans la liste d'URL, vous ne pouvez pas utiliser les symboles spéciaux « * » (astérisque) et « ? » (point d'interrogation). Par exemple, les adresses de page Web avec plusieurs domaines de niveau supérieur doivent être entrées manuellement (*pageexemple.com*, *pageexemple.fr*, etc.). Lorsque vous entrez un domaine dans la liste, tout le contenu situé dans ce domaine et dans ses sous-domaines (ex. *sous.pageexemple.com*) sera bloqué ou autorisé en fonction du choix d'action basée sur l'URL.

Remarque : bloquer ou autoriser une page Web spécifique peut s'avérer plus approprié que de bloquer ou autoriser une catégorie complète de pages Web. Soyez vigilant lorsque vous modifiez ces paramètres et ajoutez une catégorie/ page Web à la liste.

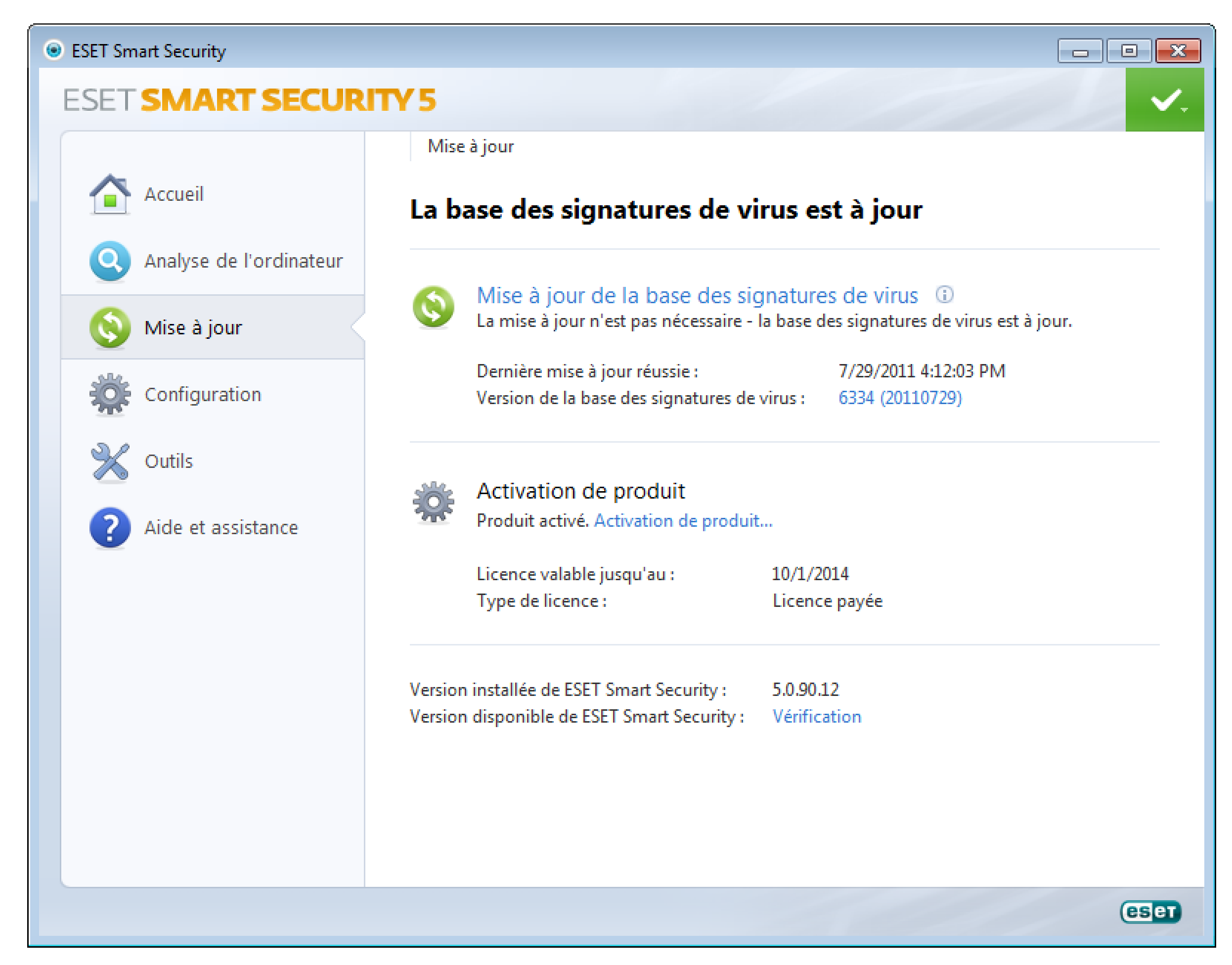
4.5 Mise à jour du programme

La mise à jour régulière d'ESET Smart Security est la meilleure méthode pour bénéficier le niveau maximum de sécurité de votre ordinateur. Le module de mise à jour veille à ce que le programme soit toujours à jour de deux façons : en mettant à jour la base des signatures de virus et en mettant à jour les composants système.

En cliquant sur **Mettre à jour** dans la fenêtre principale du programme, vous pouvez connaître l'état actuel de la mise à jour, notamment la date et l'heure de la dernière mise à jour. Vous pouvez également savoir si une mise à jour est nécessaire. La fenêtre Mise à jour contient également la version de la base des signatures de virus. Cette indication numérique est un lien actif vers le site Web d'ESET, qui répertorie toutes les signatures ajoutées dans cette mise à jour.

Par ailleurs, il est possible de démarrer manuellement la mise à jour à l'aide de l'option **Mettre à jour la base des signatures de virus**. La mise à jour de la base des signatures de virus et celle des composants du programme sont des opérations importantes de la protection totale contre les attaques des codes malveillants. Il convient donc d'apporter une grande attention à leur configuration et à leur fonctionnement. Si vous n'avez pas saisi les détails (nom d'utilisateur et mot de passe) de la licence pendant l'installation, vous pouvez les indiquer lors de la mise à jour pour accéder aux serveurs de mise à jour ESET.

REMARQUE : vos nom d'utilisateur et mot de passe sont fournis par ESET après l'achat d'ESET Smart Security.



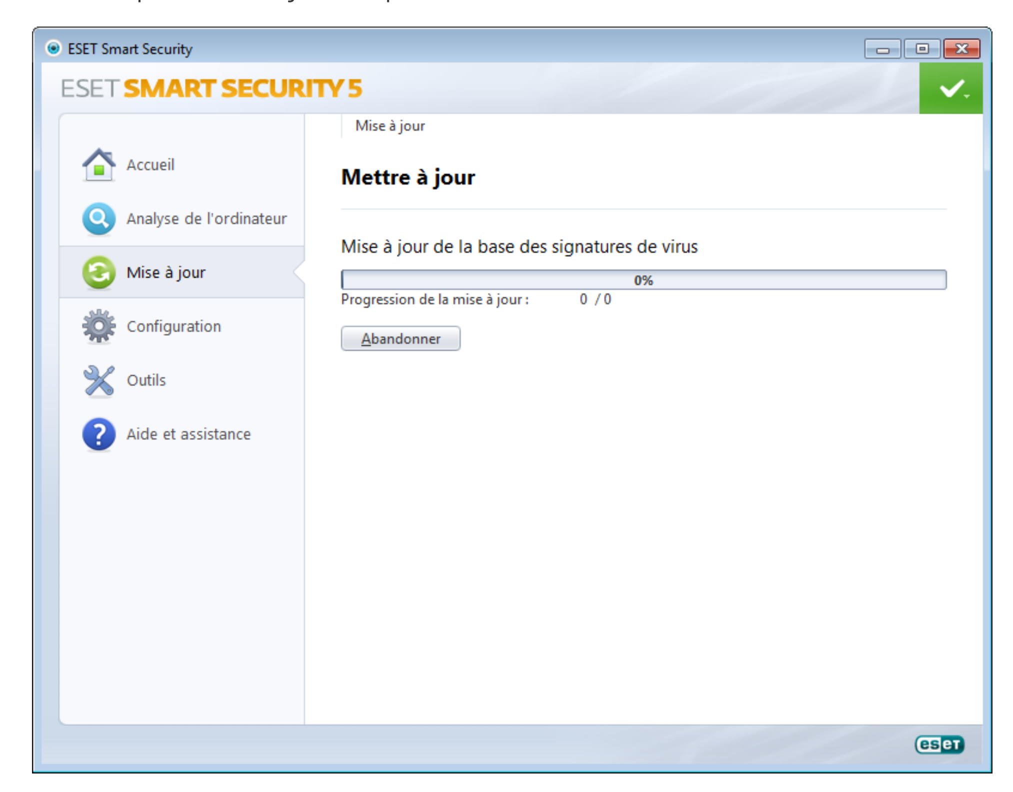
Dernière mise à jour réussie - Date de la dernière mise à jour. Vérifiez qu'il s'agit d'une date récente indiquant que la base des signatures de virus est à jour.

Version de la base des signatures de virus - Numéro de base des signatures de virus ; il s'agit également d'un lien actif vers le site Web d'ESET. Cliquez ici pour afficher la liste de toutes les signatures ajoutées dans la mise à jour.

Cliquez sur **Vérification** pour détecter la version disponible la plus récente de ESET Smart Security.

Processus de mise à jour

Une fois que vous avez cliqué sur le bouton **Mettre à jour la base des signatures de virus**, le processus de téléchargement commence. La barre de progression qui s'affiche indique le temps de téléchargement restant. Pour interrompre la mise à jour, cliquez sur **Abandonner**.

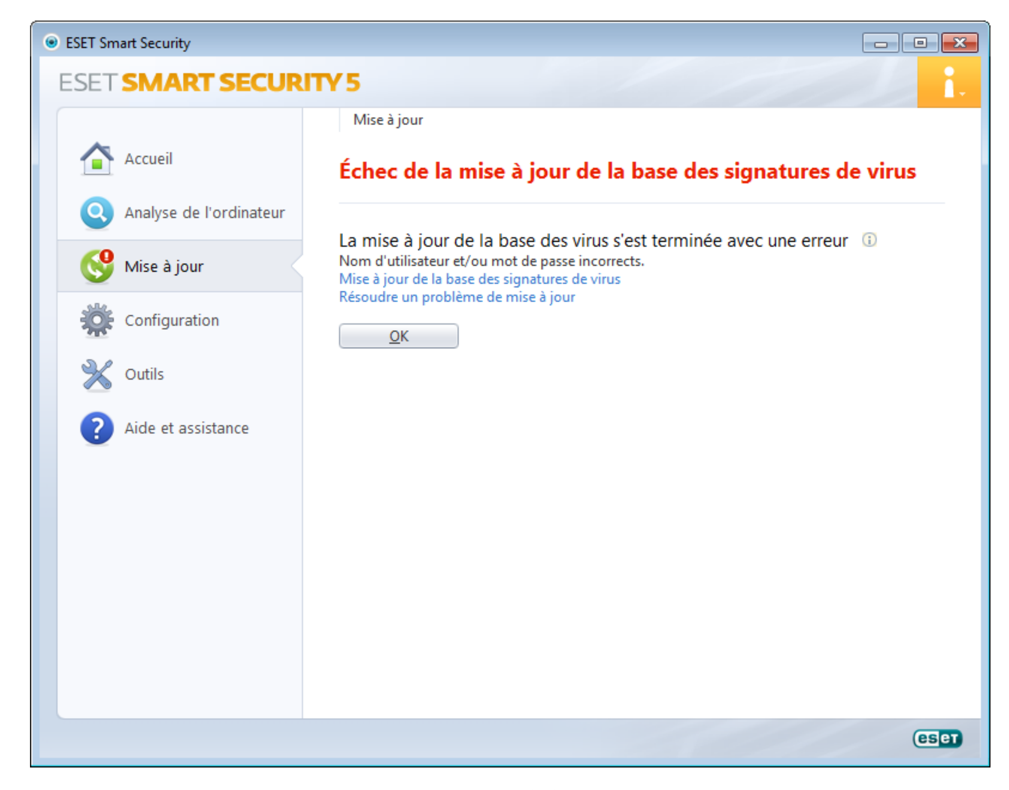


Important : dans des circonstances normales, lorsque les mises à jour sont téléchargées correctement, le message **Mise à jour non nécessaire - la base des signatures de virus installée est à jour** s'affiche dans la fenêtre **Mise à jour**. Si ce n'est pas le cas, le programme n'est pas à jour et le risque d'infection est accru. Veillez à mettre à jour la base des signatures de virus dès que possible. Dans d'autres circonstances, l'un des messages d'erreur suivants s'affiche :

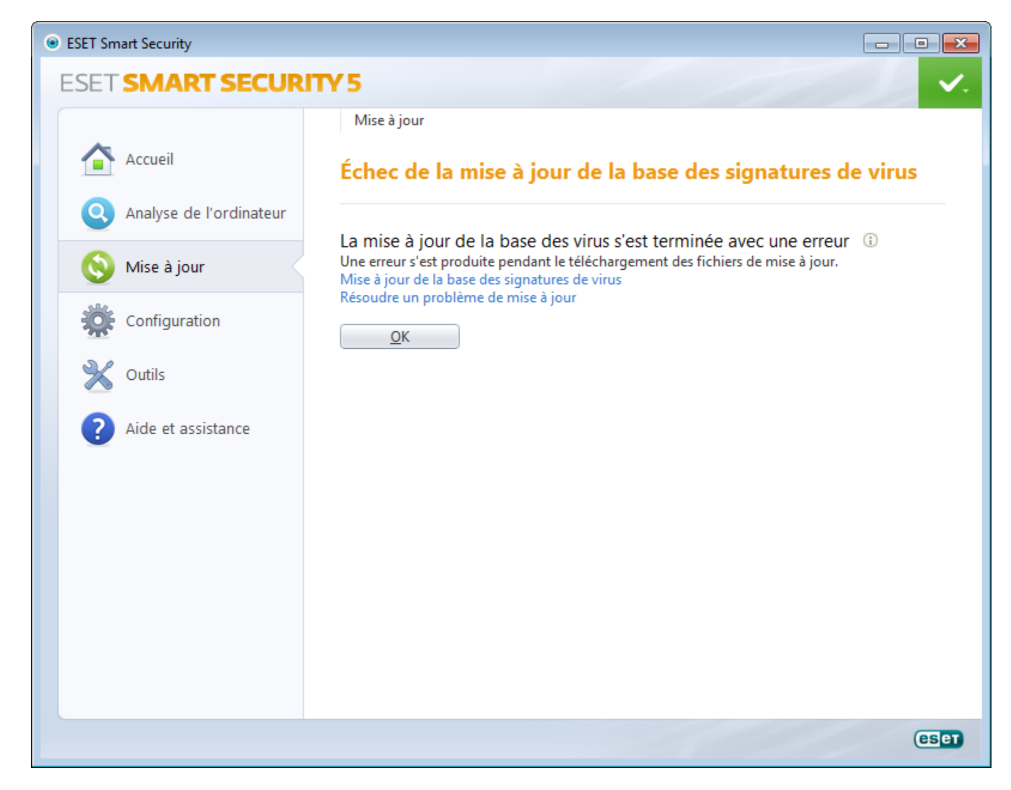
La base des signatures de virus n'est plus à jour - Cette erreur apparaît après plusieurs tentatives infructueuses de mise à jour de la base des signatures de virus. Nous vous conseillons de vérifier les paramètres de mise à jour. Cette erreur provient généralement de l'entrée incorrecte de données d'authentification ou de la configuration incorrecte des paramètres de connexion.

La notification précédente concerne les deux messages **Échec de la mise à jour de la base des signatures de virus** sur les mises à jour infructueuses :

1. **Nom d'utilisateur et/ou mot de passe incorrect(s)** - Le nom d'utilisateur et le mot de passe entrés pour la configuration des mises à jour sont incorrects. Nous vous recommandons de vérifier vos données d'authentification. La fenêtre Configuration avancée (cliquez sur **Configuration** dans le menu principal et sur **Accéder à la configuration avancée...**, ou appuyez sur la touche F5 de votre clavier) comporte d'autres options de mise à jour. Cliquez sur **Mettre à jour** > **Mettre à jour** dans l'arborescence de configuration avancée pour entrer de nouveaux nom d'utilisateur et mot de passe.



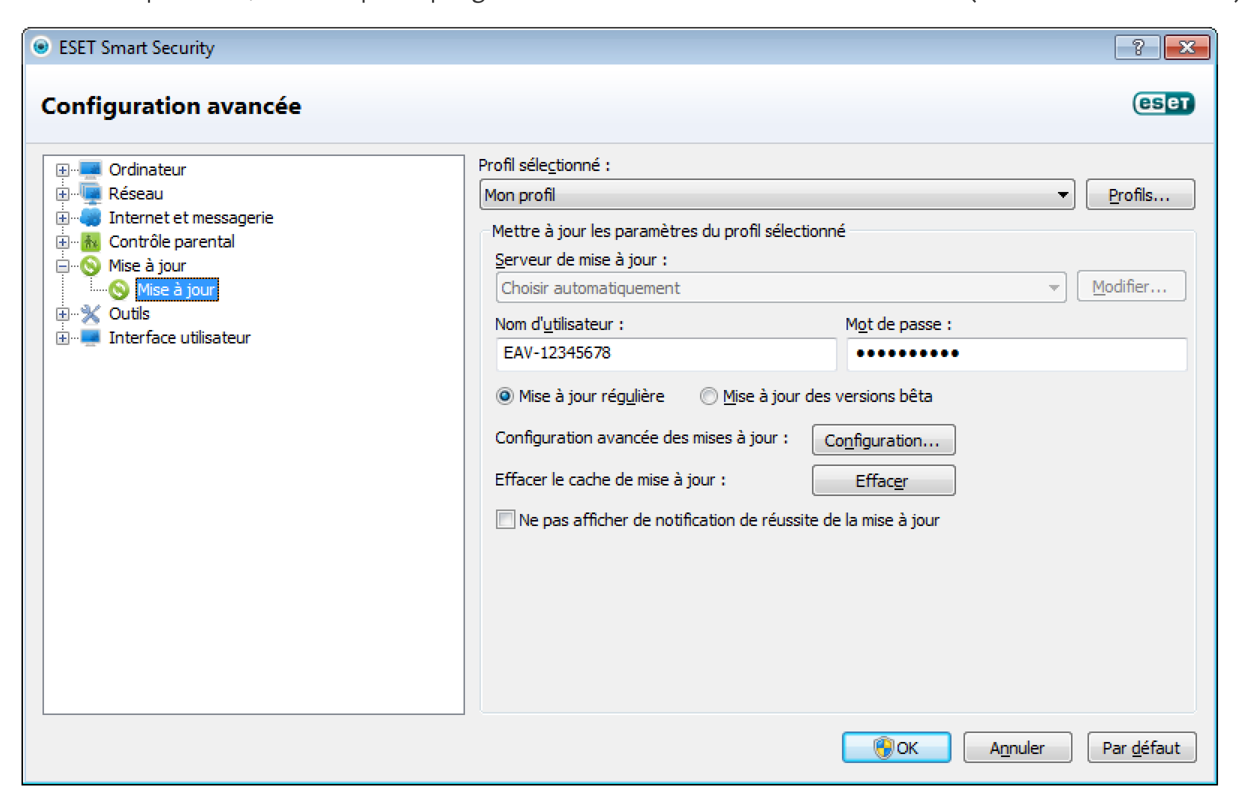
2. **Une erreur s'est produite pendant le téléchargement des fichiers de mise à jour** - L'erreur peut être due à des paramètres de connexion Internet incorrects. Nous vous recommandons de vérifier votre connectivité à Internet (en ouvrant un site Web dans votre navigateur). Si le site Web ne s'ouvre pas, cela est probablement dû au fait qu'aucune connexion à Internet n'est établie ou que votre ordinateur a des problèmes de connectivité. Consultez votre fournisseur de services Internet si vous n'avez pas de connexion Internet active.



4.5.1 Configuration des mises à jour

Les options de configuration des mises à jour sont accessibles dans la **Configuration avancée** complète (touche F5), en cliquant sur **Mettre à jour** > **Mettre à jour**. Cette section permet de spécifier les informations concernant les sources des mises à jour, telles que les serveurs de mise à jour et les données d'authentification donnant accès à ces serveurs. Par défaut, le menu déroulant **Serveur de mise à jour** est défini sur l'option **Choisir automatiquement**, ce qui garantit que les fichiers de mise à jour sont téléchargés automatiquement depuis le serveur ESET en utilisant le moins de ressources réseau possible.

Il est essentiel de remplir tous les paramètres avec précision afin de télécharger correctement les mises à jour. Si vous utilisez un pare-feu, vérifiez que le programme est autorisé à accéder à Internet (communication HTTP).



Le profil de mise à jour utilisé est affiché dans le menu déroulant **Profil sélectionné**. Cliquez sur **Profils...** pour créer un nouveau profil.

L'authentification des serveurs de mise à jour est basée sur le **nom d'utilisateur** et le **mot de passe** générés et qui vous ont été envoyés après l'achat. En cas d'utilisation d'un serveur miroir local, la vérification dépend de sa configuration. Par défaut, aucune vérification n'est exigée : les champs **Nom d'utilisateur** et **Mot de passe** restent vides.

Les mises à jour des versions bêta (l'option **Mise à jour des versions bêta**) ont subi toutes les phases internes de test et seront généralement disponibles très prochainement. Vous pouvez activer ces versions bêta afin d'accéder aux dernières méthodes de détection et aux derniers correctifs. Toutefois, ces versions ne sont peut-être pas suffisamment stables pour être utilisées en permanence et NE DOIVENT PAS être utilisées sur des serveurs de production et des stations de travail qui exigent les plus grandes disponibilité et stabilité. La liste des modules en cours est disponible dans **Aide et assistance** > **À propos d'ESET Smart Security**. Il est recommandé pour les utilisateurs non avertis de conserver la sélection par défaut de l'option **Mise à jour régulière**.

Cliquez sur le bouton **Configuration...** à côté de l'option **Configuration avancée des mises à jour** pour afficher une fenêtre des options de mise à jour avancée.

En cas de problème de mise à jour, cliquez sur le bouton **Effacer...** pour vider le dossier contenant les fichiers temporaires de mise à jour.

Ne pas afficher de notification de réussite de la mise à jour - Désactive les notifications qui apparaissent dans la barre d'état système, dans l'angle inférieur droit de l'écran. Cette option est utile si une application ou un jeu s'exécute en mode plein écran. Veuillez noter que le Mode joueur désactive toutes les notifications.

4.5.1.1 Profils de mise à jour

Les profils de mise à jour ne peuvent pas être créés pour différentes configurations et tâches de mise à jour. La création de profils de mise à jour est particulièrement utile pour les utilisateurs mobiles qui peuvent créer un autre profil correspondant aux propriétés de connexion Internet qui changent régulièrement.

Le menu déroulant **Profil sélectionné** affiche le profil sélectionné ; il est défini par défaut sur **Mon profil**. Pour créer un nouveau profil, cliquez sur les boutons **Profils...** et **Ajouter...**, puis indiquez votre propre **nom du profil**. Lors de la création d'un nouveau profil, vous pouvez copier les paramètres d'un profil existant en le sélectionnant dans le menu déroulant **Copier les paramètres depuis le profil**.

Dans la fenêtre de configuration du profil, vous pouvez indiquer le serveur de mise à jour dans la liste des serveurs disponibles ou encore ajouter un nouveau serveur. La liste des serveurs de mise à jour existants est accessible dans le menu déroulant **Serveur de mise à jour**. Pour ajouter un nouveau serveur de mise à jour, cliquez sur **Modifier...** dans la section **Mettre à jour les paramètres du profil sélectionné**, puis cliquez sur le bouton **Ajouter**.

4.5.1.2 Configuration avancée des mises à jour

Pour afficher la configuration avancée des mises à jour, cliquez sur le bouton **Configuration...**. Les options de configuration avancée de mise à jour englobent les options **Mode de mise à jour**, **Proxy HTTP** et **Réseau local**.

4.5.1.2.1 Mode de mise à jour

L'onglet **Mode de mise à jour** contient les options concernant la mise à jour des composants du programme. Le programme vous permet de prédéfinir son comportement lorsqu'une nouvelle mise à niveau de composant programme est disponible.

Les mises à jour des composants du programme offrent de nouvelles fonctionnalités ou modifient les versions précédentes. Cette mise à jour peut s'effectuer sans intervention de l'utilisateur ou après sa notification. Le redémarrage de l'ordinateur peut être nécessaire après la mise à jour des composants du programme. Dans la section **Mise à jour des composants du programme**, trois options sont disponibles :

- **Ne jamais mettre à jour les composants du programme** - Aucune mise à jour des composants du programme n'a lieu. Cette option convient aux serveurs, car ces derniers ne peuvent généralement être redémarrés qu'en cas de maintenance.
- **Toujours mettre à jour les composants du programme** - Les mises à jour de composants du programme sont téléchargées et installées automatiquement. Notez que le redémarrage du système peut être nécessaire.
- **Demander avant de télécharger les composants du programme** - Option par défaut. Vous êtes invité à confirmer ou à refuser les mises à jour de composants de programme lorsqu'elles sont disponibles.

Après l'installation d'une mise à jour de composants du programme, il est peut-être nécessaire de redémarrer l'ordinateur afin de bénéficier de toutes les fonctionnalités des modules. La section **Redémarrer après une mise à jour des composants du programme** vous permet de sélectionner l'une des options suivantes :

- **Ne jamais redémarrer** - Vous n'êtes pas invité à redémarrer le système, même si c'est obligatoire. Notez qu'il n'est pas recommandé de sélectionner cette option, car l'ordinateur pourrait ne pas bien fonctionner jusqu'au prochain redémarrage.
- **Proposer le redémarrage de l'ordinateur si nécessaire** - Option par défaut. Après la mise à jour de composants du programme, une boîte de dialogue apparaît et invite à redémarrer l'ordinateur.
- **Si nécessaire, redémarrer sans notification** - Après la mise à niveau des composants du programme, l'ordinateur redémarre (si nécessaire).

REMARQUE : la sélection de l'option la plus appropriée dépend du poste de travail sur lequel les paramètres sont appliqués. Notez qu'il existe des différences entre les postes de travail et les serveurs. Par exemple, le redémarrage automatique d'un serveur après une mise à niveau du programme peut causer de sérieux dommages.

Si l'option **Demander avant de télécharger une mise à jour** est cochée, une notification s'affiche lorsqu'une nouvelle mise à jour est disponible.

Si la taille du fichier de mise à jour est supérieure à la valeur spécifiée dans le champ **Demander si un fichier de mise à jour a une taille supérieure à**, le programme affiche une notification.

L'option **Vérifier régulièrement la dernière version du produit** active la tâche planifiée correspondante (voir Planificateur).

4.5.1.2.2 Serveur proxy

Pour accéder aux options de configuration du serveur proxy pour un profil de mise à jour donné, cliquez sur **Mise à jour** dans la configuration avancée complète (F5), puis sur le bouton **Configuration...** à droite de l'option **Configuration avancée des mises à jour**. Cliquez sur l'onglet **Proxy HTTP** et sélectionnez l'une des trois options suivantes :

- **Utiliser les paramètres globaux de serveur proxy**
- **Ne pas utiliser de serveur proxy**
- **Connexion via un serveur proxy**

L'option **Utiliser les paramètres globaux de serveur proxy** utilise les options de configuration de serveur proxy déjà indiquées dans la branche **Outils** > **Serveur proxy** de la configuration avancée complète.

Sélectionnez l'option **Ne pas utiliser de serveur proxy** pour indiquer qu'aucun serveur proxy ne sera utilisé pour la mise à jour d'ESET Smart Security.

L'option **Connexion via un serveur proxy** doit être sélectionnée si :

- Un serveur proxy doit être utilisé pour mettre à jour ESET Smart Security et ce serveur doit être différent de celui indiqué dans les paramètres globaux (**Outils** > **Serveur proxy**). Si c'est le cas, des paramètres supplémentaires doivent être spécifiés : l'adresse du **Serveur proxy**, le **Port** de communication, ainsi que le **nom d'utilisateur** et le **mot de passe** du serveur proxy, si nécessaire.
- Les paramètres de serveur proxy n'ont pas été définis globalement, mais ESET Smart Security se connecte à un serveur proxy pour les mises à jour.
- Votre ordinateur est connecté à Internet par l'intermédiaire d'un serveur proxy. Les paramètres sont pris dans Internet Explorer pendant l'installation du programme, mais s'ils sont modifiés par la suite (par exemple en cas de changement de fournisseur de services Internet), vérifiez que les paramètres du proxy HTTP sont corrects dans la fenêtre. Dans le cas contraire, le programme ne pourra pas se connecter aux serveurs de mise à jour.

L'option par défaut pour le serveur proxy est **Utiliser les paramètres globaux de serveur proxy**.

REMARQUE : les données d'authentification telles que **Nom d'utilisateur** et **Mot de passe** permettent d'accéder au serveur proxy. Ne remplissez ces champs que si un nom d'utilisateur et un mot de passe sont requis. Notez que ces champs ne sont pas ceux du mot de passe/nom d'utilisateur d'ESET Smart Security et ne doivent être remplis que si vous savez que vous avez besoin d'un mot de passe pour accéder à Internet via un serveur proxy.

4.5.1.2.3 Connexion au réseau local

Lors de mise à jour depuis un serveur local sur un système d'exploitation NT, une authentification est par défaut exigée pour chaque connexion réseau. Dans la plupart des cas, un compte système local n'a pas suffisamment de droits pour accéder au dossier miroir (ce dossier contient des copies des fichiers de mise à jour). Dans ce cas, entrez un nom d'utilisateur et un mot de passe dans la section de configuration des mises à jour ou spécifiez un compte avec lequel le programme peut accéder au serveur de mise à jour (miroir).

Pour configurer un compte de ce type, cliquez sur l'onglet **Réseau local**. La section **Se connecter au réseau local comme** propose les options **Compte système (par défaut)**, **Utilisateur actuel** et **Utilisateur spécifié**.

Sélectionnez l'option **Compte système (par défaut)** afin d'utiliser le compte système pour l'authentification. Normalement, aucun traitement d'authentification n'a lieu si les données d'authentification ne sont pas fournies dans la section de configuration des mises à jour.

Pour s'assurer que le programme s'authentifie à l'aide du compte de l'utilisateur connecté, sélectionnez **Utilisateur actuel**. L'inconvénient de cette solution est que le programme ne peut pas se connecter au serveur de mise à jour si aucun utilisateur n'est connecté.

Sélectionnez **Utilisateur spécifié** si vous voulez que le programme utilise un compte utilisateur spécifié pour l'authentification. Utilisez cette méthode si la connexion avec le compte système échoue. Notez que le compte de l'utilisateur spécifié doit avoir accès au dossier des fichiers de mise à jour du serveur local. Dans le cas contraire, le programme ne pourrait pas établir la connexion nécessaire pour télécharger les mises à jour.

Avertissement : Si l'une des options **Utilisateur actuel** ou **Utilisateur spécifié** est activée, une erreur peut se produire en cas de changement de l'identité du programme pour l'utilisateur souhaité. C'est pour cette raison que nous recommandons d'entrer les données d'authentification du réseau local dans la section de configuration des mises à jour. Dans cette section de configuration des mises à jour, les données d'authentification doivent être entrées comme suit : *nom_de_domaine\utilisateur* (dans le cas d'un groupe de travail, entrez *nom_de_groupe_de_travail\utilisateur*) et le mot de passe. La mise à jour de la version HTTP du serveur local n'exige aucune authentification.

Sélectionnez l'option **Déconnecter du serveur après la mise à jour** si la connexion au serveur reste active, même après

le téléchargement des mises à jour.

4.5.2 Comment créer des tâches de mise à jour

Vous pouvez déclencher les mises à jour manuellement en cliquant sur **Mettre à jour la base des signatures de virus** dans la fenêtre principale qui s'affiche lorsque vous cliquez sur **Mettre à jour** dans le menu principal.

Les mises à jour peuvent également être exécutées sous forme de tâches planifiées. Pour configurer une tâche planifiée, cliquez sur **Outils** > **Planificateur**. Par défaut, les tâches suivantes sont activées dans ESET Smart Security :

- **Mise à jour automatique régulière**
- **Mise à jour automatique après une connexion commutée**
- **Mise à jour automatique après ouverture de session utilisateur**

Chaque tâche de mise à jour peut être modifiée selon les besoins de l'utilisateur. Outre les tâches de mise à jour par défaut, vous pouvez en créer des nouvelles avec vos propres paramètres. Pour plus d'informations sur la création et la configuration des tâches de mise à jour, reportez-vous à la section Planificateur.

4.6 Outils

Le menu **Outils** comprend des modules qui contribuent à simplifier l'administration du programme et offrent des options supplémentaires aux utilisateurs expérimentés.



Ce menu comprend les éléments suivants :

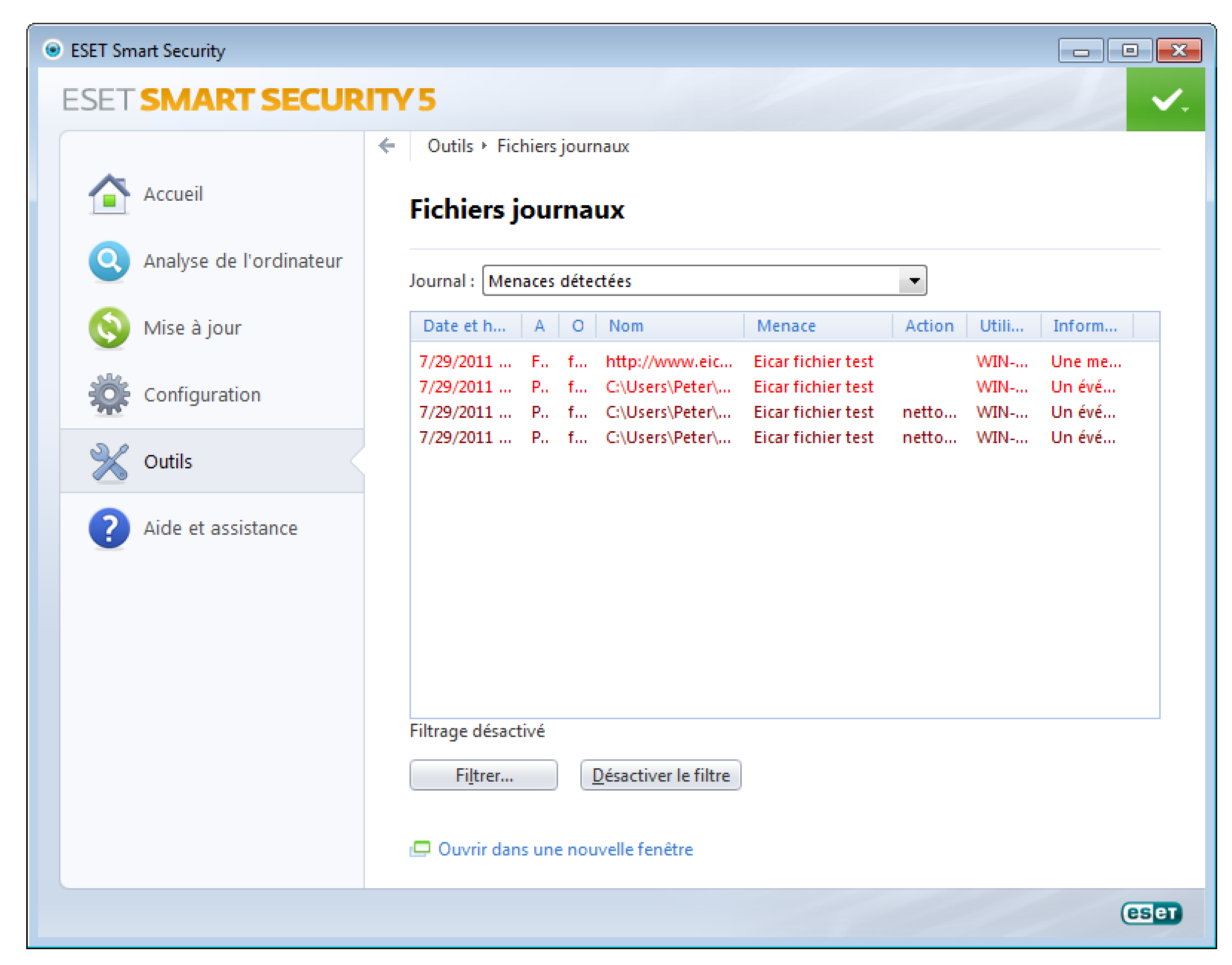
- Fichiers journaux
- Statistiques de protection
- Surveiller l'activité
- Processus en cours
- Planificateur
- Quarantaine
- Connexions réseau
- ESET SysInspector

Soumettre le fichier pour analyse - Permet de soumettre un fichier suspect pour analyse aux laboratoires d'ESET. La boîte de dialogue qui s'affiche lorsque vous cliquez sur cette option est décrite dans la section Soumission de fichiers pour analyse.

ESET SysRescue - Lance l'assistant de création ESET SysRescue.

4.6.1 Fichiers journaux

Les fichiers journaux contiennent tous les événements importants qui se sont produits et fournissent un aperçu des menaces détectées. La consignation représente un puissant outil pour l'analyse système, la détection de menaces et le dépannage. La consignation est toujours active en arrière-plan sans interaction de l'utilisateur. Les informations sont enregistrées en fonction des paramètres de détail actifs. Il est possible de consulter les messages texte et les journaux directement à partir de l'environnement ESET Smart Security, ainsi que d'archiver les journaux.



Vous pouvez accéder aux fichiers journaux depuis la fenêtre principale du programme en cliquant sur **Outils** > **Fichiers journaux**. Sélectionnez le type de journal à partir du menu déroulant **Journal**. Les journaux suivants sont disponibles :

- **Menaces détectées** - Le journal des menaces contient des informations sur les infiltrations détectées par les modules ESET Smart Security. Ces informations comprennent l'heure de détection, le nom de l'infiltration, l'emplacement, l'action exécutée et le nom de l'utilisateur connecté au moment où l'infiltration a été détectée. Double-cliquez sur une entrée du journal pour afficher son contenu dans une fenêtre distincte.

- **Événements** - Toutes les actions importantes exécutées par ESET Smart Security sont enregistrées dans le journal des événements. Le journal des événements contient des informations sur les événements qui se sont produits dans

le programme. Il permet aux administrateurs système et aux utilisateurs de résoudre des problèmes. Les informations qu'il contient peuvent aider à trouver une solution à un problème qui s'est produit dans le programme.

- **Analyse de l'ordinateur** - Cette fenêtre affiche toutes les analyses effectuées, qu'elles soient manuelles ou planifiées. Chaque ligne correspond à un seul contrôle d'ordinateur. Double-cliquez sur une entrée pour afficher les détails de l'analyse correspondante.
- **HIPS** - Contient des entrées de règles spécifiques qui ont été marquées pour enregistrement. Le protocole affiche l'application qui a appelé l'opération, le résultat (si la règle a été autorisée ou bloquée), ainsi que le nom de la règle créée.
- **Pare-feu personnel** - Le journal du pare-feu contient toutes les attaques distantes détectées par le pare-feu personnel. Il comprend des renseignements sur les attaques subies par votre ordinateur. La colonne *Événement* répertorie les attaques détectées. La colonne *Source* fournit des informations sur l'attaquant. La colonne *Protocole* indique le protocole de communication utilisé pour l'attaque. L'analyse du journal de pare-feu permet de détecter à temps les tentatives d'infiltration du système et d'éviter tout accès non autorisé à votre système.
- **Protection antispam** - Contient des entrées relatives aux messages marqués comme spam.
- **Contrôle parental** - Affiche les pages Web bloquées ou autorisées par le contrôle parental. Les colonnes *Type de correspondance* et *Valeurs de correspondance* indiquent comment les règles de filtrage ont été appliquées.

Dans chaque section, vous pouvez copier les informations affichées dans chaque section directement dans le Presse-papiers (à l'aide du raccourci clavier Ctrl + C) en sélectionnant l'entrée souhaitée, puis en cliquant sur le bouton **Copier**. Pour sélectionner plusieurs entrées, vous pouvez utiliser les touches CTRL et MAJ.

Vous pouvez afficher le menu contextuel d'une entrée en cliquant sur cette entrée avec le bouton droit de la souris. Le menu contextuel permet d'accéder aux options suivantes :

- **Filtrer les entrées du même type** - Si vous activez ce filtre, vous voyez uniquement les enregistrements du même type (diagnostics, avertissement, ...).
- **Filtrer.../Rechercher...** - Après avoir cliqué sur cette option, vous pouvez définir les critères de filtrage dans la fenêtre **Filtrage des journaux** qui s'affiche.
- **Désactiver le filtre** - Supprime tous les paramètres du filtre (comme décrit ci-dessus).
- **Copier tout** - Copie des informations sur toutes les entrées de la fenêtre.
- **Supprimer/Supprimer tout** - Supprime les entrées sélectionnées ou toutes les entrées affichées. Vous devez disposer des privilèges d'administrateur pour effectuer cette action.
- **Exporter** - Exporte les informations sur les entrées au format XML.
- **Dérouler journal** - Laissez cette option activée pour que les anciens journaux défilent automatiquement et pour consulter les journaux actifs dans la fenêtre **Fichiers journaux**.

4.6.1.1 Maintenance des journaux

La configuration des fichiers journaux de ESET Smart Security est accessible à partir de la fenêtre principale du programme. Cliquez sur **Configuration** > **Accéder à la configuration avancée...** > **Outils** > **Fichiers journaux**. La section Fichiers journaux permet de définir la manière dont les journaux sont gérés. Le programme supprime automatiquement les anciens fichiers journaux pour gagner de l'espace disque. Les options suivantes peuvent être spécifiées pour les fichiers journaux :

Supprimer automatiquement les entrées - Les entrées des journaux plus anciennes que le nombre de jours spécifiés dans **Supprimer les entrées vieilles de plus de X jours** seront automatiquement supprimées.

Optimiser automatiquement les fichiers journaux – Si cette fonction est activée, les fichiers journaux sont automatiquement défragmentés si le pourcentage est plus grand que la valeur spécifiée dans le champ **Si le nombre d'entrées inutilisées dépasse (%)**.

Cliquez sur **Optimiser maintenant** pour démarrer la défragmentation des fichiers journaux. Au cours de ce processus, toutes les entrées vides du journal sont supprimées, ce qui améliore les performances et accélère le traitement des journaux. Cette amélioration se constate notamment si les journaux comportent un grand nombre d'entrées.

Verbosité minimale des journaux - Spécifie le niveau minimum de verbosité des événements à consigner.

- **Diagnostic** - Consigne toutes les informations nécessaires au réglage du programme et de toutes les entrées ci-dessus.
- **Entrées informatives** - Enregistre tous les messages d'information, y compris les messages de mises à jour réussies et toutes les entrées ci-dessus.
- **Avertissements** - Enregistre les erreurs critiques, les erreurs et les messages d'avertissement.
- **Erreurs** - Consigne les erreurs du type *« Erreur de téléchargement du fichier »* et erreurs critiques.
- **Critique** - Répertorie toutes les erreurs critiques (erreur de démarrage de la protection antivirus, pare-feu personnel, etc...).

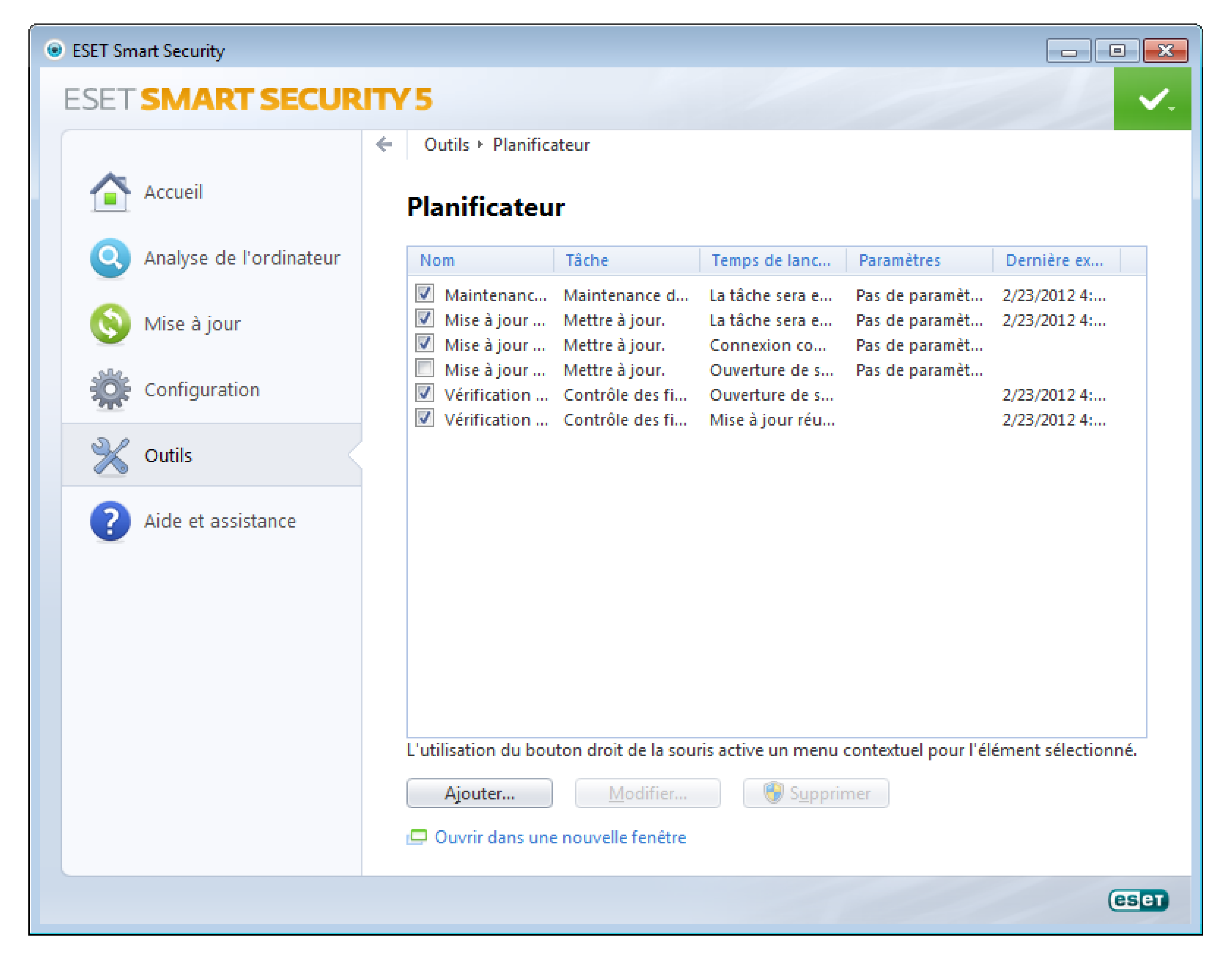
Cliquez sur le bouton **Filtre par défaut...** pour ouvrir la fenêtre **Filtrage des journaux**. Cochez les types d'entrées à afficher dans les journaux et cliquez sur **OK**.

4.6.2 Planificateur

Le planificateur gère et lance les tâches planifiées qui ont été préalablement définies et configurées.

Le planificateur est accessible depuis la fenêtre principale de ESET Smart Security, dans **Outils** > **Planificateur**. Le **planificateur** contient la liste de toutes les tâches planifiées, des propriétés de configuration telles que la date et l'heure prédéfinies, ainsi que le profil d'analyse utilisé.

Il sert à planifier les tâches suivantes : la mise à jour de la base des signatures de virus, l'analyse, le contrôle des fichiers de démarrage du système et la maintenance des journaux. Vous pouvez ajouter ou supprimer des tâches dans la fenêtre principale du planificateur (cliquez sur **Ajouter...** ou **Supprimer** dans la partie inférieure). Cliquez avec le bouton droit dans la fenêtre du planificateur pour effectuer les actions suivantes : afficher des informations détaillées, exécuter la tâche immédiatement, ajouter une nouvelle tâche et supprimer une tâche existante. Utilisez les cases à cocher au début de chaque entrée pour activer/désactiver les tâches.



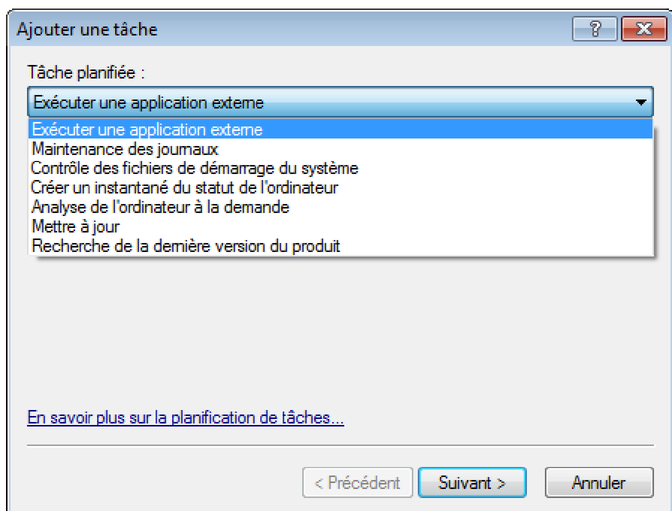
Par défaut, les tâches planifiées suivantes sont affichées dans le **planificateur** :

- **Maintenance des journaux**
- **Mise à jour automatique régulière**
- **Mise à jour automatique après une connexion commutée**
- **Mise à jour automatique après ouverture de session utilisateur**
- **Recherche régulière de la dernière version du produit** (voir Mode de mise à jour)
- **Vérification des fichiers de démarrage** (après l'ouverture de session de l'utilisateur)
- **Vérification des fichiers de démarrage** (après la mise à jour réussie de la base des signatures de virus)

Pour modifier la configuration d'une tâche planifiée existante (par défaut ou définie par l'utilisateur), cliquez avec le bouton droit sur la tâche et cliquez sur **Modifier...**. Vous pouvez également sélectionner la tâche à modifier et cliquer sur le bouton **Modifier...**

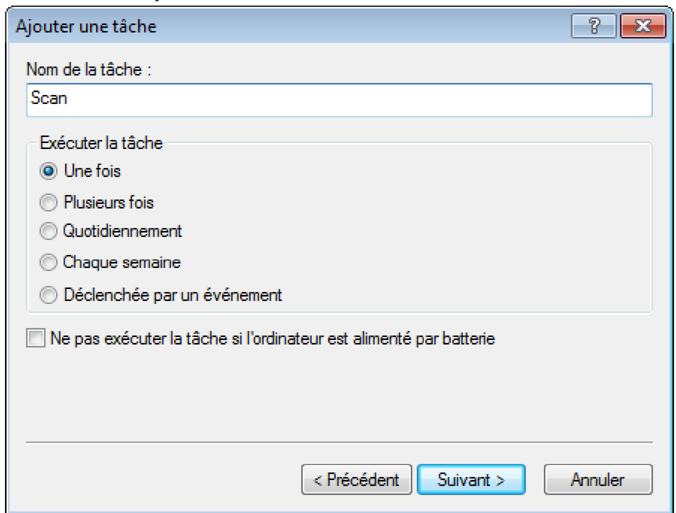
Ajout d'une nouvelle tâche

1. Cliquez sur **Ajouter...** dans la partie inférieure de la fenêtre.
2. Sélectionnez la tâche souhaitée dans le menu déroulant.



3. Saisissez le nom de la tâche, puis choisissez une des options de planification :

   - **Une fois** - La tâche est exécutée une fois, à la date et à l'heure prédéfinies.
   - **Plusieurs fois** - La tâche est exécutée aux intervalles indiqués (en heures).
   - **Quotidiennement** - La tâche est exécutée tous les jours à l'heure définie.
   - **Chaque semaine** - La tâche est exécutée une ou plusieurs fois par semaine, au(x) jour(s) et à l'heure indiqués.
   - **Déclenchée par un événement** - La tâche est exécutée après un événement particulier.



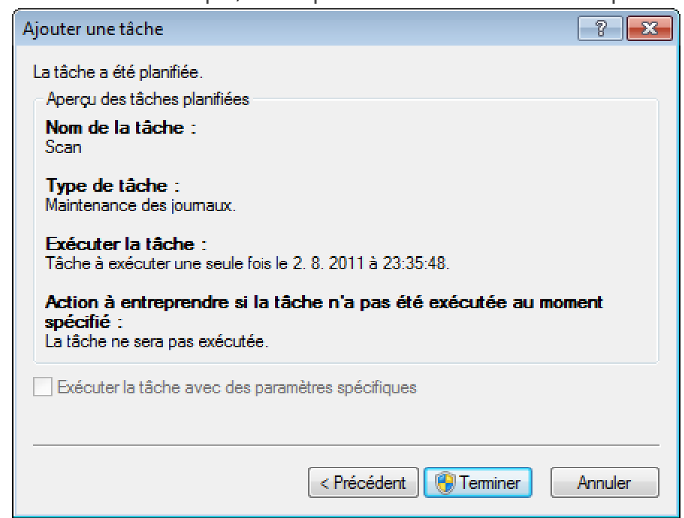
4. En fonction de l'option de périodicité que vous choisissez à l'étape précédente, l'une des boîtes de dialogue suivantes apparaît :

   - **Une fois** - La tâche est exécutée à la date et à l'heure prédéfinies.
   - **Plusieurs fois** - La tâche est exécutée aux intervalles indiqués.
   - **Quotidiennement** - La tâche est exécutée tous les jours à l'heure définie.
   - **Chaque semaine** - La tâche est exécutée à l'heure et au jour prédéfinis.

5. Si la tâche n'a pas pu être exécutée au moment défini, vous pouvez désigner le moment auquel elle doit être réexécutée :

   - Patienter jusqu'à la prochaine heure planifiée
   - Exécuter la tâche dès que possible
   - Exécuter la tâche immédiatement si le temps écoulé depuis la dernière exécution est supérieur à -- heures.

6. À la dernière étape, vous pouvez réviser la tâche à planifier. Cliquez sur **Terminer** pour appliquer la tâche.



4.6.2.1 Création de nouvelles tâches

Pour créer une nouvelle tâche dans le planificateur, cliquez sur le bouton **Ajouter...** ou cliquez avec le bouton droit sur la tâche et sélectionnez **Ajouter...** dans le menu contextuel. Cinq types de tâches planifiées sont disponibles :

- **Exécuter une application externe** - Permet de programmer l'exécution d'une application externe.
- **Maintenance des journaux** - Les fichiers journaux contiennent également des éléments provenant d'enregistrements supprimés. Cette tâche optimise régulièrement les entrées des fichiers journaux pour garantir leur efficacité.
- **Contrôle des fichiers de démarrage du système** - Vérifie les fichiers autorisés à s'exécuter au démarrage du système ou lors de l'ouverture de session de l'utilisateur.
- **Créer un instantané du statut de l'ordinateur** - Crée l'instantané d'ordinateur ESET SysInspector - collecte des informations détaillées sur les composants système (pilotes, applications) et évalue le niveau de risque de chacun de ces composants.
- **Analyse de l'ordinateur** - Analyse les fichiers et dossiers de votre ordinateur.
- **Mettre à jour** - Planifie une tâche de mise à jour en mettant à jour la base des signatures de virus et les modules du programme.
- **Recherche régulière de la dernière version du produit**

La tâche planifiée la plus fréquente étant la **mise à jour**, nous allons expliquer comment ajouter une nouvelle tâche de mise à jour.

Dans le menu déroulant **Tâche planifiée**, sélectionnez **Mettre à jour**. Cliquez sur **Suivant** et saisissez le nom de la tâche dans le champ **Nom de la tâche**. Sélectionnez la fréquence de la tâche. Les options disponibles sont les suivantes : **Une fois**, **Plusieurs fois**, **Quotidiennement**, **Hebdo** et **Déclenchée par un événement**. Utilisez l'option **Ne pas exécuter la tâche si l'ordinateur est alimenté par batterie** pour diminuer les ressources système lorsque l'ordinateur portable fonctionne sur batterie. Selon la fréquence sélectionnée, vous êtes invité à choisir différents paramètres de mise à jour. Vous pouvez définir ensuite l'action à entreprendre si la tâche ne peut pas être effectuée ou terminée à l'heure planifiée. Les trois options suivantes sont disponibles :

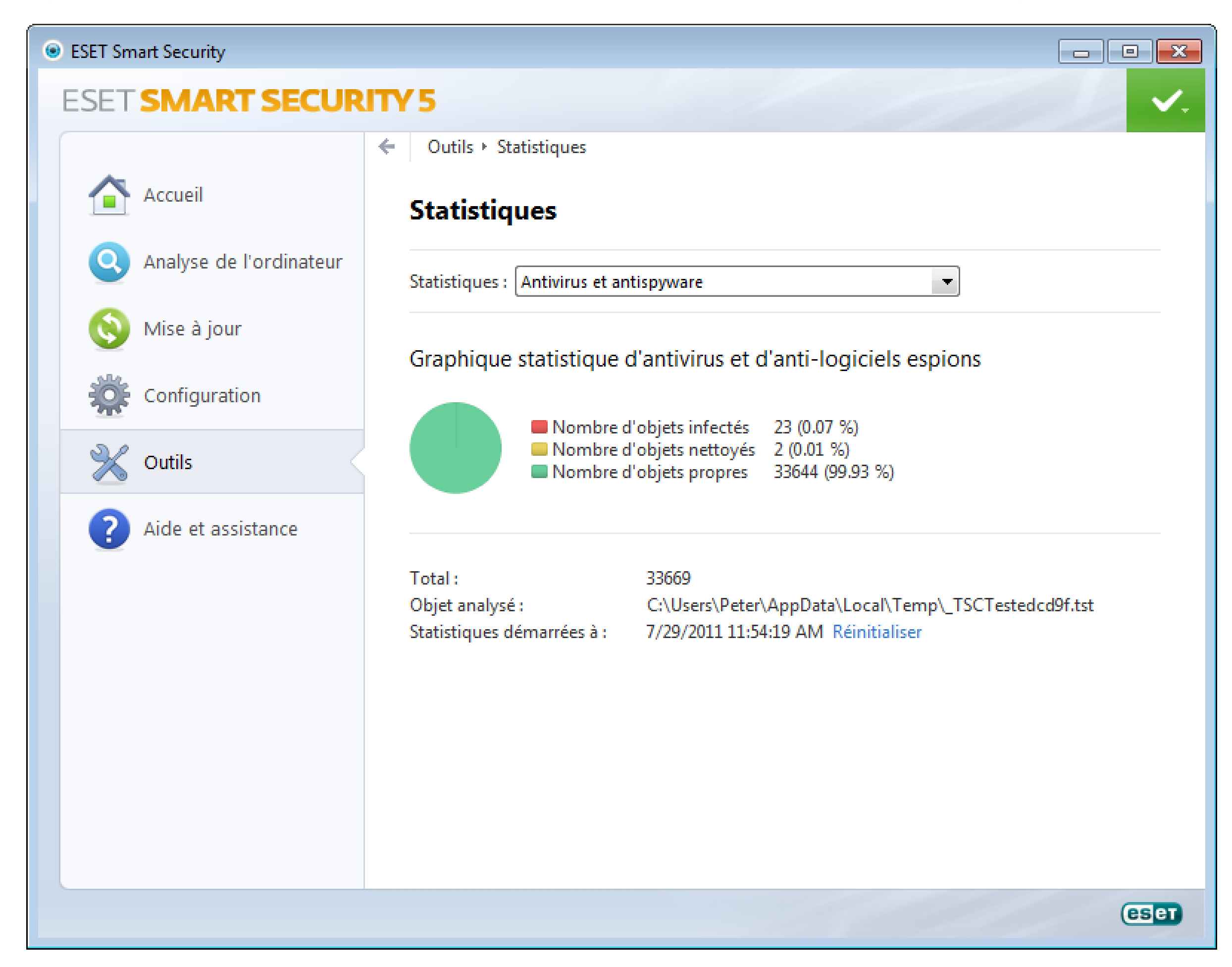
- **Patienter jusqu'à la prochaine heure planifiée**
- **Exécuter la tâche dès que possible**
- **Exécuter la tâche immédiatement si le temps écoulé depuis la dernière exécution dépasse l'intervalle spécifié** (l'intervalle peut être défini à l'aide de la zone de liste déroulante Intervalle minimal entre deux tâches)

La prochaine étape affiche dans une fenêtre un résumé complet de la tâche planifiée courante ; l'option **Exécuter la tâche avec des paramètres spécifiques** doit être automatiquement activée. Cliquez sur le bouton **Terminer**.

La boîte de dialogue qui apparaît permet de sélectionner les profils à utiliser pour la tâche planifiée. L'utilisateur peut spécifier un profil principal et un profil secondaire qui sera utilisé si la tâche ne peut s'exécuter à l'aide du profil principal. Confirmez en cliquant sur **OK** de la fenêtre **Profils de mise à jour**. La nouvelle tâche planifiée est ajoutée à la liste des tâches planifiées.

4.6.3 Statistiques de protection

Pour afficher un graphique des données statistiques relatives aux modules de protection d'ESET Smart Security, cliquez sur **Outils** > **Statistiques**. Dans le menu déroulant **Statistiques**, sélectionnez le module de protection souhaité pour afficher le graphique et la légende correspondants. Si vous faites glisser le pointeur de la souris sur un élément de la légende, seules les données correspondant à cet élément sont représentées dans le graphique.



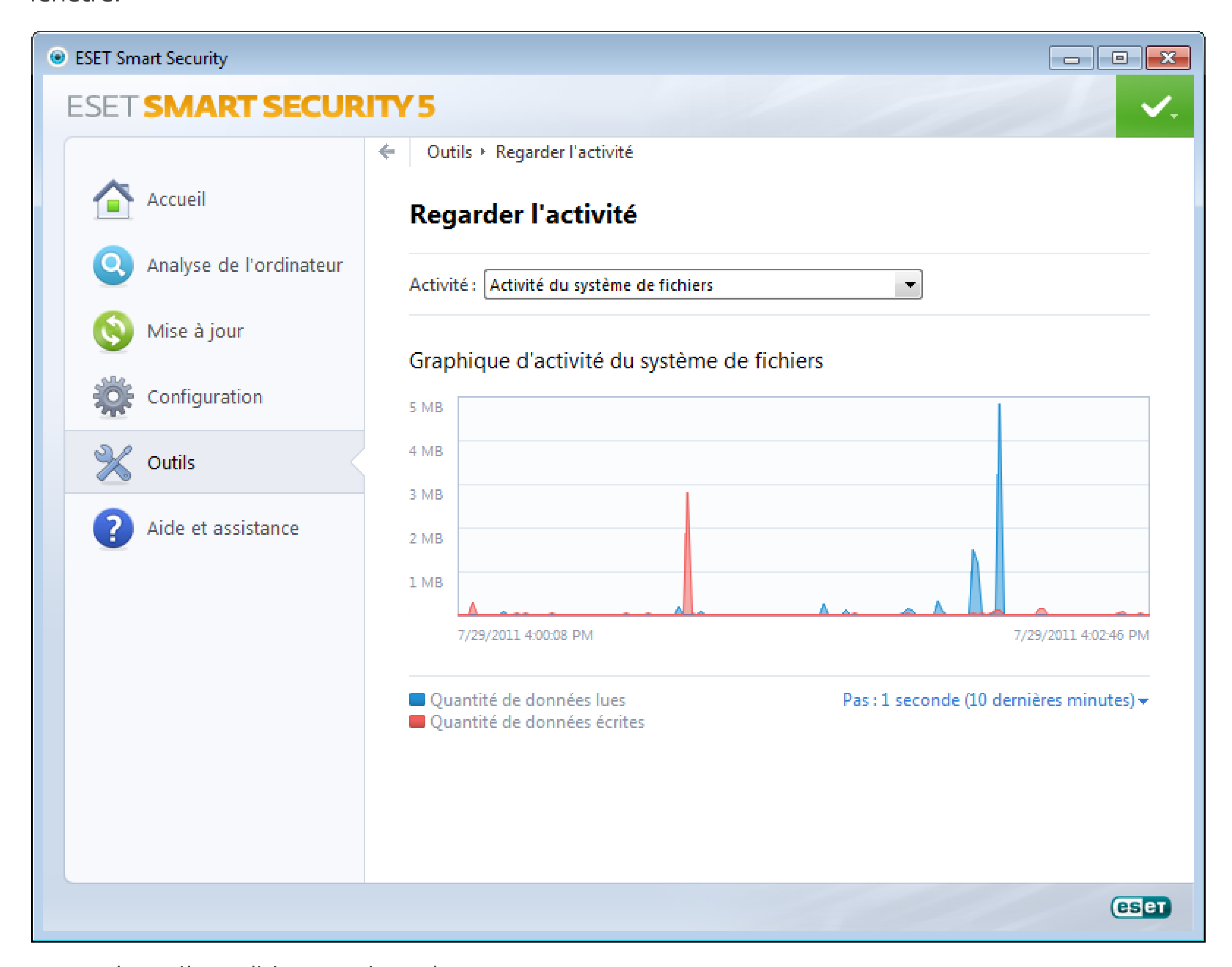
Les graphiques statistiques suivants sont disponibles :

- **Protection antivirus et antispyware** - Affiche le nombre d'objets infectés et nettoyés.
- **Protection du système de fichiers** - Affiche uniquement les objets lus ou écrits dans le système de fichiers.
- **Protection du client de messagerie** - Affiche uniquement les objets envoyés ou reçus par les clients de messagerie.
- **Protection de l'accès au Web et antihameçonnage** - Affiche uniquement les objets téléchargés par des navigateurs Web.
- **Protection antispam du client messagerie** - Affiche l'historique des statistiques de blocage du courrier indésirable depuis le dernier démarrage.

Sous les graphiques statistiques, vous pouvez voir le nombre total d'objets analysés, le dernier objet analysé et l'horodatage des statistiques. Cliquez sur **Réinitialiser** pour supprimer toutes les informations statistiques.

4.6.4 Regarder l'activité

Pour voir l'**activité actuelle du système de fichiers** sous forme graphique, cliquez sur **Outils** > **Surveiller l'activité**. Au bas du graphique figure une chronologie qui enregistre en temps réel l'activité du système de fichiers sur la base de l'intervalle sélectionné. Pour changer l'échelle, cliquez sur l'option **Pas 1...** située dans la partie inférieure droite de la fenêtre.



Les options disponibles sont les suivantes :

- **Pas : 1 seconde (10 dernières minutes)** - Le graphique est actualisé toutes les secondes et la chronologie couvre les 10 dernières minutes
- **Pas : 1 minute (24 dernières heures)** - Le graphique est actualisé toutes les secondes et la chronologie couvre les 24 dernières heures
- **Pas : 1 heure (dernier mois)** - Le graphique est actualisé toutes les heures et la chronologie couvre le dernier mois
- **Pas : 1 heure (mois sélectionné)** - Le graphique est actualisé toutes les heures et la chronologie couvre les X mois sélectionnés.

L'axe vertical **Graphique d'activité du système de fichiers** représente les données lues (en bleu) et les données écrites (en rouge). Les deux valeurs sont exprimées en Ko (kilo-octets)/Mo/Go. Si vous faites glisser le curseur de la souris sur les données lues ou écrites dans la légende sous le graphique, celui-ci n'affiche que les données relatives à ce type d'activité.

Vous pouvez également sélectionner **Activité réseau** dans le menu déroulant **Activité**. L'affichage et les options du graphique pour l'**Activité du système de fichiers** et l'**Activité du réseau** sont identiques, à la différence près que, pour cette dernière, les données reçues (en bleu) et envoyées (en rouge) sont présentées.

4.6.5 ESET SysInspector

ESET SysInspector est une application qui inspecte méticuleusement votre ordinateur, réunit des informations détaillées sur les composants système, tels que pilotes et applications installés, connexions réseau ou entrées de registre importantes, puis évalue le niveau de risque de chaque composant. Ces informations peuvent aider à déterminer la cause d'un comportement suspect du système pouvant être dû à une incompatibilité logicielle ou matérielle, ou à une infection par un logiciel malveillant.

La fenêtre SysInspector affiche les informations suivantes relatives aux journaux créés :

- **Heure** - Heure de création du journal.
- **Commentaire** - Bref commentaire.
- **Utilisateur** - Nom de l'utilisateur qui a créé le journal.
- **État** - État de création du journal.

Les actions disponibles sont les suivantes :

- **Comparer** - Compare deux journaux existants.
- **Créer...** - Crée un journal. Veuillez patienter jusqu'à ce que le journal ESET SysInspector soit prêt (l'option **État** indique Créé).
- **Supprimer** - Supprime les journaux sélectionnés de la liste.

En cliquant avec le bouton droit de la souris sur un ou plusieurs journaux sélectionnés, vous ouvrez un menu contextuel qui donne accès aux options suivantes :

- **Afficher** - Ouvre le journal sélectionné dans ESET SysInspector (équivaut à double-cliquer sur un journal).
- **Supprimer tout** - Supprime tous les journaux.
- **Exporter...** - Exporte le journal dans un fichier *.xml* ou un fichier *.xml* compressé .

4.6.6 ESET Live Grid

ESET Live Grid (la nouvelle génération d'ESET ThreatSense.Net) est un système d'alerte avancé qui vous protège des nouvelles menaces en se basant sur la réputation. Le laboratoire ESET utilise le flux en temps réel d'informations concernant les menaces issues du service de cloud computing pour maintenir les défenses à jour. Vous bénéficiez d'un niveau de protection constant. L'utilisateur peut s'informer de la réputation des processus et des fichiers en cours d'exécution depuis l'interface du programme ou à partir d'un menu contextuel comprenant des informations supplémentaires mises à disposition par ESET Live Grid. Deux options sont possibles :

1. Vous pouvez décider de ne pas activer ESET Live Grid. Vous ne perdez rien de la fonctionnalité du logiciel et vous bénéficiez toujours la meilleure protection que nous offrons.
2. Vous pouvez configurer ESET Live Grid afin d'envoyer des informations anonymes qui concernent les nouvelles menaces et indiquent l'endroit où se trouve le code dangereux. Ce fichier peut être envoyé à ESET pour une analyse détaillée. En étudiant ces menaces, ESET améliore ses capacités à détecter les menaces.

Le système ESET Live Grid collecte sur votre ordinateur des informations concernant les nouvelles menaces détectées. Ces informations comprennent un échantillon ou une copie du fichier dans lequel la menace est apparue, le chemin et le nom du fichier, la date et l'heure, le processus par lequel la menace est apparue sur votre ordinateur et des informations sur le système d'exploitation de votre ordinateur.

Par défaut, ESET Smart Security est configuré pour demander une confirmation avant de soumettre les fichiers suspects au laboratoire d'ESET pour une analyse détaillée. Les fichiers ayant une extension définie (*.doc* ou *.xls* par exemple) sont toujours exclus. Vous pouvez également ajouter d'autres extensions si vous ou votre entreprise souhaitez éviter d'envoyer certains fichiers.

Le menu de configuration ESET Live Grid propose différentes options permettant d'activer et de désactiver ESET Live Grid. Ce système sert à soumettre les fichiers suspects aux laboratoires d'ESET et à fournir des informations statistiques anonymes. Cette option est accessible depuis la fenêtre Configuration avancée en cliquant sur **Outils** > **ESET Live Grid**.

Participer à ESET Live Grid (recommandé) - Active et désactive ESET Live Grid. Ce système sert à soumettre les fichiers suspects aux laboratoires d'ESET et à fournir des informations statistiques anonymes.

Ne pas soumettre de statistiques - Sélectionnez cette option si vous ne souhaitez pas soumettre d'informations anonymes concernant votre ordinateur depuis ESET Live Grid. Ces informations concernent les nouvelles menaces détectées. Il peut s'agir du nom de l'infiltration, de la date et de l'heure de la détection, de la version d'ESET Smart Security et d'informations sur la version du système d'exploitation de votre ordinateur et ses paramètres régionaux. Les statistiques sont normalement fournies au serveur d'ESET une ou deux fois par jour.

Ne pas soumettre de fichiers - Les fichiers suspects, qui ressemblent à des infiltrations par leur contenu ou leur comportement, ne sont pas envoyés pour analyse à ESET par le biais de la technologie ESET Live Grid.

Configuration avancée... - Ouvre une fenêtre avec d'autres paramètres ESET Live Grid.

Si vous avez déjà utilisé le système ESET Live Grid et l'avez désactivé, il est possible qu'il reste des paquets de données à envoyer. Même après la désactivation, ces paquets seront transmis à ESET à la prochaine occasion. Par la suite, plus aucun paquet ne sera créé.

4.6.6.1 Fichiers suspects

L'onglet **Fichiers** dans la configuration avancée ESET Live Grid permet de configurer le mode de soumission des menaces au laboratoire de recherche sur les menaces d'ESET pour analyse.

Si vous trouvez un fichier suspect, vous pouvez le soumettre à notre laboratoire de recherche sur les menaces pour analyse. S'il s'agit d'une application malveillante, sa détection est ajoutée à la prochaine mise à jour de la base des signatures de virus.

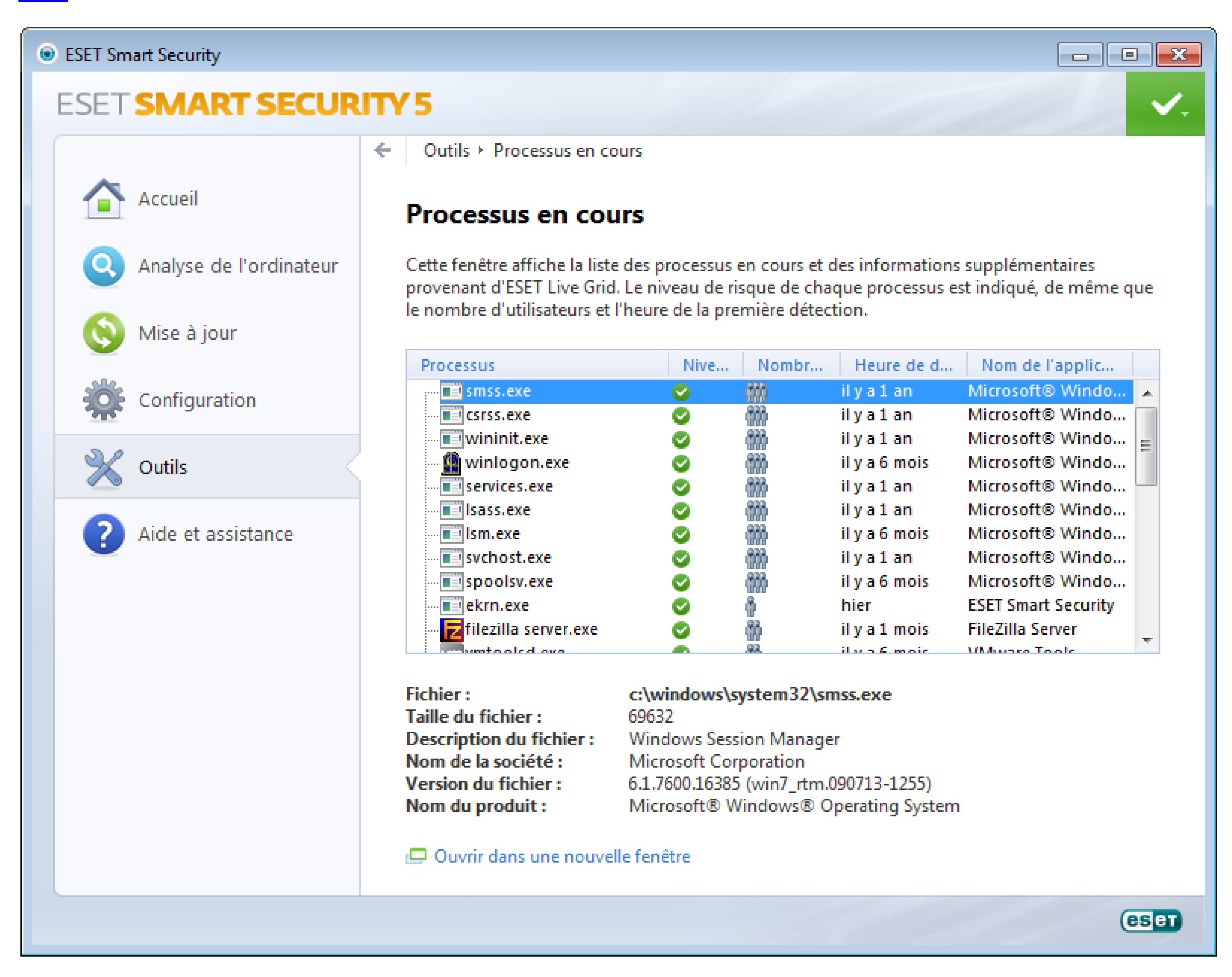
Filtre d'exclusion - Cette option permet d'exclure certains fichiers/dossiers de la soumission. Les fichiers de la liste ne seront jamais envoyés aux laboratoires d'ESET pour analyse, même s'ils contiennent un code suspect. Par exemple, il peut être utile d'exclure des fichiers qui peuvent comporter des informations confidentielles, telles que des documents ou des feuilles de calcul. Les fichiers les plus ordinaires sont exclus par défaut (.doc, etc.). Vous pouvez ajouter des fichiers à la liste des fichiers exclus si vous le souhaitez.

Adresse électronique de contact (facultatif) - Votre adresse électronique peut être incluse avec les fichiers suspects. Nous pourrons l'utiliser pour vous contacter si des informations complémentaires sont nécessaires pour l'analyse. Notez que vous ne recevrez pas de réponse d'ESET, sauf si des informations complémentaires s'avèrent nécessaires.

Sélectionnez l'option **Activer la journalisation** pour créer un journal d'événements permettant d'enregistrer les soumissions des fichiers et des informations statistiques. Il permet de consigner les fichiers ou statistiques envoyés dans le Journal des événements.

4.6.7 Processus en cours

Les processus en cours affichent les programmes ou processus en cours d'exécution sur votre ordinateur et informe ESET immédiatement et en permanence de l'existence de nouvelles infiltrations. ESET Smart Security fournit des informations détaillées sur l'exécution des processus afin de protéger les utilisateurs à l'aide de la technologie ESET Live Grid.



Processus - Nom de l'image du programme ou du processus en cours d'exécution sur l'ordinateur. Vous pouvez également utiliser le Gestionnaire de tâches pour afficher tous les processus en cours d'exécution sur votre ordinateur. Vous pouvez ouvrir le Gestionnaire de tâches en cliquant avec le bouton droit de la souris sur une zone vide de la barre des tâches, puis en cliquant sur Gestionnaire de tâches, ou en appuyant sur les touches Ctrl+Maj+Échap du clavier.

Niveau de risque - Dans la majorité des cas, ESET Smart Security et la technologie ESET Live Grid attribuent des niveaux de risque aux objets (fichiers, processus, clés de registre, etc.) sur la base d'une série de règles heuristiques qui examinent les caractéristiques de chaque objet, puis qui évaluent le potentiel d'activité malveillante. Cette analyse heuristique attribue aux objets un niveau de risque allant de 1 - OK (vert) à 9 - Risqué (rouge).

REMARQUE : les applications connues marquées OK (vert) sont saines (répertoriées dans la liste blanche) et sont exclues de l'analyse, ce qui améliore la vitesse de l'analyse d'ordinateur à la demande ou de la protection du système en temps réel sur votre ordinateur.

Nombre d'utilisateurs - Nombre d'utilisateurs utilisant une application donnée. Ces informations sont collectées par la technologie ESET Live Grid.

Temps de découverte - Durée écoulée depuis la détection de l'application par la technologie ESET Live Grid.

REMARQUE : Une application marquée avec le niveau de sécurité Inconnu (orange) n'est pas nécessairement un logiciel malveillant. Il s'agit généralement d'une nouvelle application. Si un fichier vous semble suspect, vous pouvez le soumettre pour analyse au laboratoire ESET. Si le fichier s'avère être une application malveillante, sa détection sera ajoutée à l'une des prochaines mises à jour.

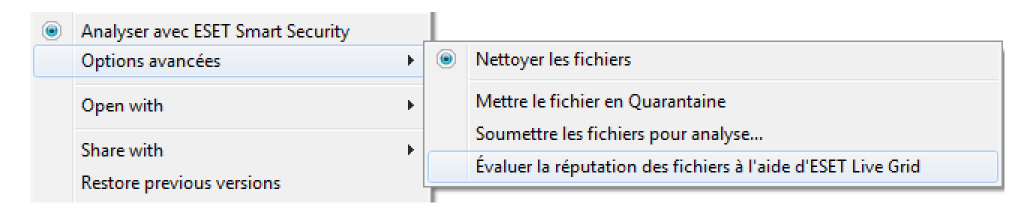
Nom de l'application - Nom d'un programme ou d'un processus.

Ouvrir dans une nouvelle fenêtre - Les informations concernant les processus en cours d'exécution s'affichent dans une nouvelle fenêtre.

Lorsque vous cliquez sur une application située au bas de la fenêtre, les informations suivantes apparaissent dans la partie inférieure de la fenêtre :

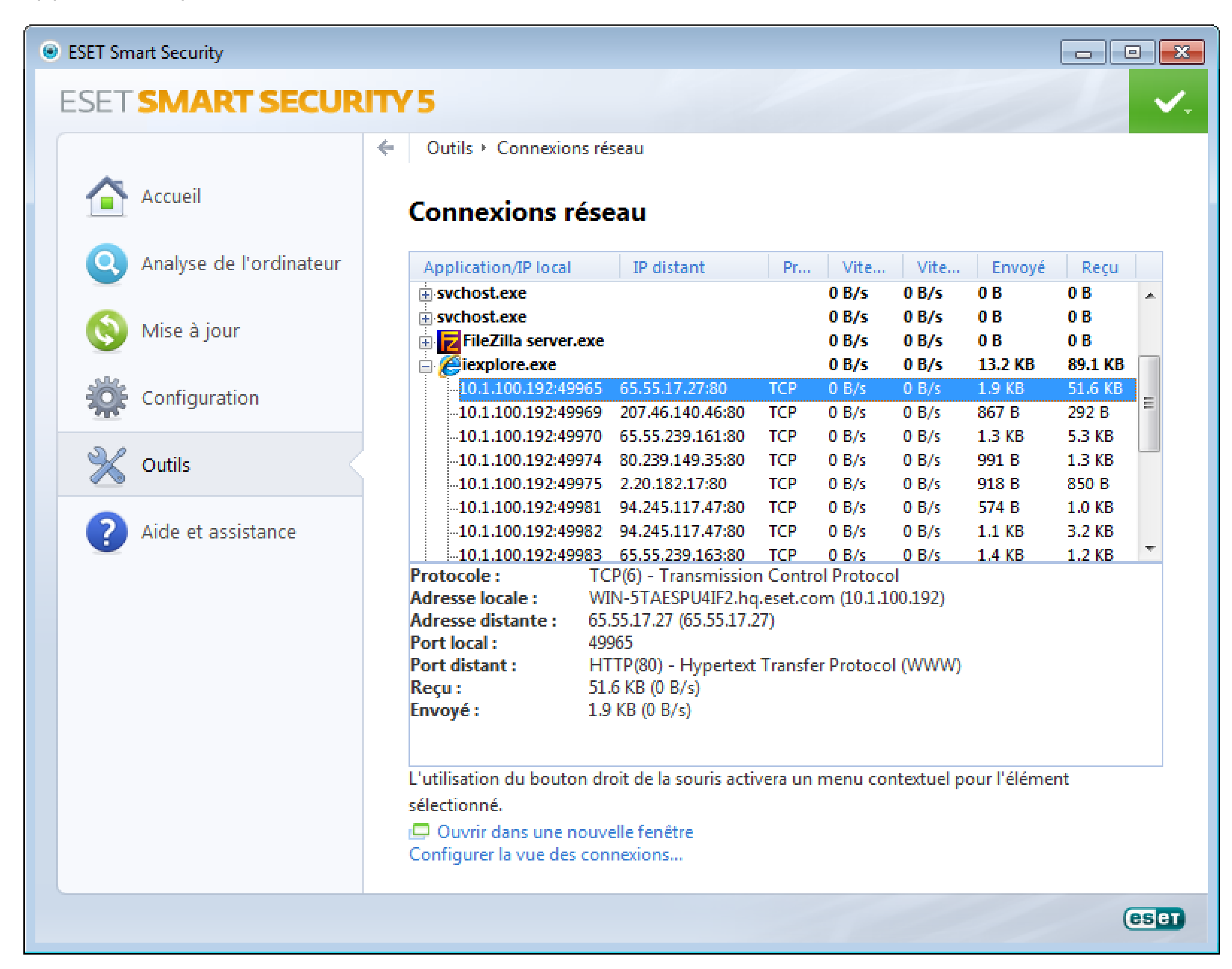
- **Fichier** - Emplacement de l'application sur l'ordinateur.
- **Taille du fichier** - Taille du fichier en o (octets).
- **Description du fichier** - Caractéristiques du fichier basées sur la description émanant du système d'exploitation.
- **Nom de la société** - Nom du fournisseur ou du processus de l'application.
- **Version du fichier** - Informations fournies par l'éditeur de l'application.
- **Nom du produit** - Nom de l'application et/ou nom de l'entreprise.

REMARQUE : la réputation peut également être vérifiée sur des fichiers qui n'agissent pas en tant que programmes/processus en cours - Marquez les fichiers que vous souhaitez vérifier, cliquez dessus avec le bouton droit et, dans le menu contextuel, sélectionnez **Options avancées** > **Évaluer la réputation des fichiers à l'aide de ESET Live Grid**.



4.6.8 Connexions réseau

La section Connexions réseau présente la liste des connexions actives et en attente. Elle vous aide à contrôler toutes les applications qui établissent des connexions sortantes.



La première ligne affiche le nom de l'application et la vitesse de transfert de données. Pour afficher la liste des connexions établies par l'application (ainsi que des informations plus détaillées), cliquez sur **+**.

Application/IP locale - Nom de l'application, adresses IP locales et ports de communication.

Adresse IP distante - Adresse IP et numéro de port d'un ordinateur distant.

Protocole - Protocole de transfert utilisé.

Vitesse montante/descendante - Vitesse actuelle des données sortantes et entrantes.

Envoyé/Reçu - Quantité de données échangées sur la connexion.

Ouvrir dans une nouvelle fenêtre - Affiche les informations dans une fenêtre séparée.

L'option **Configurer la vue des connexions...** de l'écran Connexions réseau entre dans la structure de configuration avancée de cette section, vous permettant de modifier les options de vue des connexions :

Résoudre les noms - Dans la mesure du possible, toutes les adresses réseau sont affichées dans le format DNS et non dans le format d'adresse IP numérique.

Afficher uniquement les connexions avec le protocole TCP - Cette liste affiche uniquement les connexions appartenant à la suite du protocole TCP.

Afficher les connexions ayant des ports ouverts sur lesquels l'ordinateur écoute - Cette option permet d'afficher uniquement les connexions sans communication actuellement établie, mais pour lesquelles le système a ouvert un port et est en attente de connexion.

Afficher aussi les connexions à l'intérieur de l'ordinateur - Cette option permet de n'afficher que les connexions où le côté distant est un système local ; ces connexions sont appelées connexions *hôte local*.

Cliquez avec le bouton droit sur une connexion pour afficher les options supplémentaires suivantes :

Refuser la communication pour la connexion - Met fin à la connexion établie. Cette option n'est disponible que lorsque vous cliquez sur une connexion active.

Afficher les détails - Permet d'afficher les informations détaillées de la connexion sélectionnée.

Vitesse de rafraîchissement - Permet de choisir la fréquence de rafraîchissement des connexions actives.

Rafraîchir maintenant - Recharge la fenêtre des connexions réseau.

Les options suivantes ne sont disponibles que lorsque vous cliquez sur une application ou un processus, mais pas sur une connexion active :

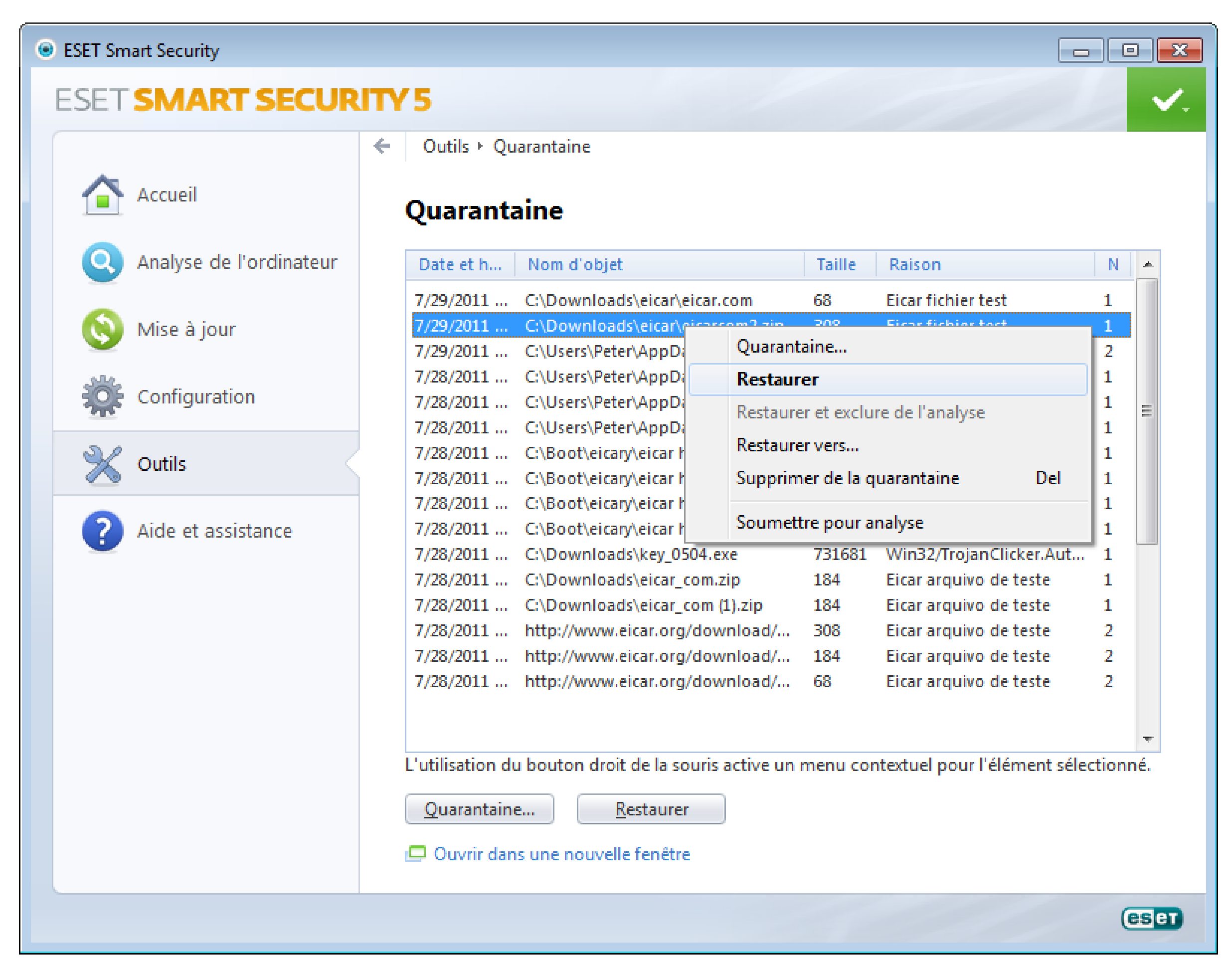
Refuser temporairement la communication pour le processus - Rejette les connexions actuelles de l'application. Si une nouvelle connexion est établie, le pare-feu utilise une règle prédéfinie. Les paramètres sont décrits dans la section Règles et zones.

Autoriser temporairement la communication pour le processus - Autorise les connexions actuelles de l'application. Si une nouvelle connexion est établie, le pare-feu utilise une règle prédéfinie. Les paramètres sont décrits dans la section Règles et zones.

4.6.9 Quarantaine

La principale fonction de la quarantaine est de stocker les fichiers infectés en toute sécurité. Les fichiers doivent être placés en quarantaine s'ils ne peuvent pas être nettoyés, s'il est risqué ou déconseillé de les supprimer ou s'ils sont détectés erronément par ESET Smart Security.

Vous pouvez choisir de mettre n'importe quel fichier en quarantaine. Cette action est conseillée si un fichier se comporte de façon suspecte, mais n'a pas été détecté par l'analyseur antivirus. Les fichiers de la quarantaine peuvent être soumis pour analyse au laboratoire de recherche d'ESET.



Les fichiers du dossier de quarantaine peuvent être visualisés dans un tableau qui affiche la date et l'heure de mise en quarantaine, le chemin d'accès à l'emplacement d'origine du fichier infecté, sa taille en octets, la raison (par exemple, objet ajouté par l'utilisateur) et le nombre de menaces (s'il s'agit d'une archive contenant plusieurs infiltrations par exemple).

Mise en quarantaine de fichiers

ESET Smart Security met automatiquement en quarantaine les fichiers supprimés (si vous n'avez pas annulé cette option dans la fenêtre d'alerte). Au besoin, vous pouvez mettre manuellement en quarantaine tout fichier suspect en cliquant sur le bouton **Quarantaine...**. Dans ce cas, le fichier d'origine n'est pas supprimé de son emplacement initial. Il est également possible d'utiliser le menu contextuel à cette fin : cliquez avec le bouton droit dans la fenêtre **Quarantaine** et sélectionnez l'option **Quarantaine...**

Restauration depuis la quarantaine

Les fichiers mis en quarantaine peuvent aussi être restaurés à leur emplacement d'origine. Pour ce faire, utilisez la fonctionnalité **Restaurer** du menu contextuel après avoir cliqué avec le bouton droit sur un fichier dans la fenêtre de quarantaine. Si un fichier est marqué comme application potentiellement indésirable, l'option **Restaurer et exclure de l'analyse** est activée. Pour en savoir plus sur ce type d'application, consultez le glossaire. Le menu contextuel propose également l'option **Restaurer vers...** qui permet de restaurer des fichiers vers un emplacement autre que celui d'origine dont ils ont été supprimés.

REMARQUE : si le programme place en quarantaine, par erreur, un fichier inoffensif, il convient de le restaurer, de l' exclure de l'analyse et de l'envoyer au service d'assistance d'ESET.

Soumission de fichiers mis en quarantaine

Si vous avez placé en quarantaine un fichier suspect non détecté par le programme ou si un fichier a été considéré par erreur comme étant infecté (par exemple par l'analyse heuristique du code) et placé en quarantaine, envoyez ce fichier au laboratoire d'ESET. Pour soumettre un fichier mis en quarantaine, cliquez avec le bouton droit sur le fichier et sélectionnez l'option **Soumettre le fichier pour analyse** dans le menu contextuel.

4.6.10 Soumission de fichiers pour analyse

La boîte de dialogue Soumission de fichiers permet d'envoyer un fichier à ESET pour analyse ; elle est accessible depuis **Outils** > **Soumettre le fichier pour analyse**. Si vous trouvez sur votre ordinateur un fichier dont le comportement est suspect, vous pouvez le soumettre au laboratoire d'ESET pour analyse. Si le fichier s'avère être une application malveillante, sa détection sera ajoutée à l'une des prochaines mises à jour.

Vous pouvez également soumettre le fichier par e-mail. Si vous préférez, compressez le ou les fichiers à l'aide de WinRAR/ZIP, protégez l'archive à l'aide du mot de passe « infected » et envoyez-la à samples@eset.com. Veillez à utiliser un objet descriptif et indiquez le plus d'informations possible sur le fichier (notez par exemple le site Internet à partir duquel vous l'avez téléchargé).

REMARQUE : avant de soumettre un fichier à ESET, assurez-vous qu'il répond à au moins l'un des critères suivants :
- le fichier n'est pas du tout détecté,
- le fichier est, à tort, détecté comme une menace.

Vous ne recevrez pas de réponse, excepté si des informations complémentaires sont nécessaires à l'analyse.

Sélectionnez dans le menu déroulant **Motif de soumission du fichie** la description correspondant le mieux à votre message :
- **Fichier suspect**,
- **Faux positif** (fichier déctecté comme infecté, mais qui ne l'est pas en réalité),
- et **Autre**.

Fichier - Chemin d'accès au fichier que vous souhaitez soumettre.

Adresse de contact - L'adresse de contact est envoyée à ESET avec les fichiers suspects. Elle pourra servir à vous contacter si des informations complémentaires sont nécessaires à l'analyse. La spécification d'une adresse de contact est facultative. Vous ne recevrez pas de réponse d'ESET, sauf si des informations complémentaires sont nécessaires à l'analyse. Nos serveurs reçoivent en effet chaque jour des dizaines de milliers de fichiers, ce qui ne permet pas de répondre à tous les envois.

4.6.11 Mises à jour système

La fonctionnalité Windows Update est un élément important de la protection des utilisateurs contre les logiciels malveillants. C'est pourquoi il est essentiel d'installer les mises à jour de Microsoft Windows dès qu'elles sont disponibles. ESET Smart Security vous informe des mises à jour manquantes en fonction du niveau que vous spécifiez. Les niveaux suivants sont disponibles :

- **Pas de mise à jour** - Aucune mise à jour système n'est proposée au téléchargement.
- **Mises à jour optionnelles** - Les mises à jour marquées comme étant faiblement prioritaires et au-dessus sont proposées au téléchargement.
- **Mises à jour recommandées** - Les mises à jour marquées comme étant courantes et au-dessus sont proposées au téléchargement.
- **Mises à jour importantes** - Les mises à jour marquées comme étant importantes et au-dessus sont proposées au téléchargement.
- **Mises à jour critiques** - Seules les mises à jour critiques sont proposées pour le téléchargement.

Cliquez sur **OK** pour enregistrer les modifications. La fenêtre Mises à jour système s'affiche après la vérification de l'état à l'aide du serveur de mise à jour. C'est pourquoi les informations de mise à jour système ne sont peut-être pas immédiatement disponibles après l'enregistrement des modifications.

4.6.12 Diagnostics

Le diagnostic fournit un fichier d'image mémoire en cas de défaillance d'une application lors des processus ESET (par exemple *ekrn*). Dès qu'une application présente une défaillance, un fichier d'image mémoire est généré. Ce fichier permet aux développeurs de déboguer et de résoudre différents problèmes ESET Smart Security. Deux types de fichier d'image mémoire sont disponibles :

- **Fichier d'image mémoire complet** - Enregistre tout le contenu de la mémoire système en cas d'arrêt inopiné de l'application. Un fichier d'image mémoire complet peut contenir des données provenant des processus en cours au moment de sa collecte.
- **Minifichier d'image mémoire** - Enregistre le plus petit ensemble d'informations utiles qui peuvent permettre d'identifier les raisons de l'arrêt inopiné de l'application. Ce type de fichier d'image mémoire peut être utile lorsque l'espace disponible est limité. Toutefois, en raison des informations limitées qui figurent dans ce fichier, les erreurs qui n'étaient pas directement provoquées par la menace, car cette dernière ne s'exécutait pas au moment du problème, risquent de ne pas être détectées par l'analyse de ce fichier.
- Sélectionnez **Ne pas générer de fichier d'image mémoire** (option par défaut) pour désactiver cette fonctionnalité.

Répertoire cible - Répertoire dans lequel est généré le fichier d'image mémoire lors de la défaillance. Cliquez sur **Ouvrir le dossier...** pour ouvrir ce répertoire dans une nouvelle fenêtre de l'*Explorateur Windows*.

4.7 Interface utilisateur

La section **Interface utilisateur** permet de configurer le comportement de l'interface utilisateur graphique du programme (GUI).

Grâce à l'outil Graphiques, vous pouvez ajuster l'apparence du programme et l'utilisation des effets.

En configurant Alertes et notifications, vous pouvez modifier le comportement des alertes concernant les menaces détectées et les notifications système. Ces alertes peuvent être personnalisées en fonction de vos besoins.

Si vous choisissez de ne pas afficher certaines notifications, ces dernières apparaissent dans les fenêtres de notification masquées. Vous pouvez vérifier leur état, afficher des détails supplémentaires ou supprimer des notifications de cette fenêtre.

Afin de bénéficier de la sécurité maximum de votre logiciel de sécurité, vous pouvez empêcher toute modification non autorisée en protégeant les paramètres par un mot de passe à l'aide de l'outil Configuration de l'accès.

Le menu contextuel est le menu qui s'affiche lorsque vous cliquez sur un objet avec le bouton droit de la souris. Utilisez cet outil pour intégrer les options ESET Smart Security dans le menu contextuel.

Le Mode joueur est utile pour les utilisateurs qui souhaitent travailler dans une application sans être interrompus par des fenêtres contextuelles, des tâches planifiées et tout autre composant qui pourrait augmenter la charge du processeur et de la mémoire RAM.

4.7.1 Graphiques

La configuration de l'interface utilisateur d'ESET Smart Security peut être modifiée de manière à adapter l'environnement de travail à vos besoins. Ces options de configuration sont accessibles depuis la branche **Interface utilisateur** > **Graphiques** de la configuration avancée complète ESET Smart Security.

Dans la section **Éléments de l'interface utilisateur**, l'**interface utilisateur graphique** doit être désactivée si les éléments graphiques ralentissent les performances de l'ordinateur ou causent d'autres problèmes. De la même manière, il est peut-être nécessaire de désactiver l'interface utilisateur graphique pour les utilisateurs malvoyants, car elle peut créer un conflit avec des applications spéciales utilisées pour la lecture de textes affichés à l'écran.

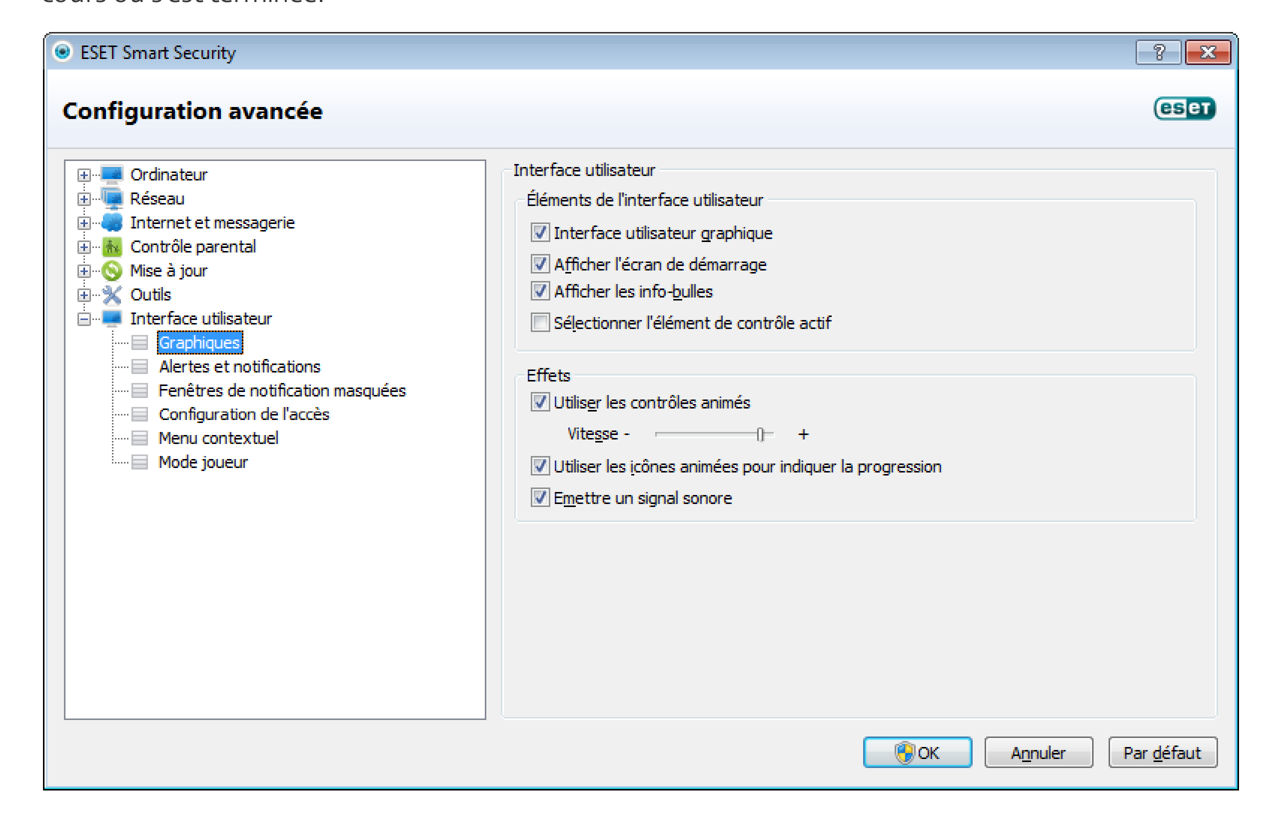
Pour désactiver l'écran de démarrage d'ESET Smart Security, désactivez l'option **Afficher l'écran de démarrage**.

Si l'option **Afficher les info-bulles** est activée, une brève description de l'option correspondante s'affiche lorsque le curseur est placé dessus. Lorsque l'option **Sélectionner l'élément de contrôle actif** est sélectionnée, le système met en évidence tout élément situé dans la zone active du curseur de la souris. L'élément mis en évidence est activé si l'utilisateur clique dessus.

Pour diminuer ou augmenter la vitesse des effets animés, sélectionnez l'option **Utiliser les contrôles animés** et déplacez le curseur **Vitesse** vers la gauche ou vers la droite.

Pour activer l'utilisation des icônes animées afin d'afficher la progression des différentes opérations, sélectionnez l'option **Utiliser les icônes animées pour indiquer la progression**.

Si vous souhaitez que le programme émette un son d'avertissement si un événement important se produit, sélectionnez **Émettre un signal sonore**. Notez qu'un son ne sera émis que lorsqu'une analyse de l'ordinateur est en cours ou s'est terminée.



4.7.2 Alertes et notifications

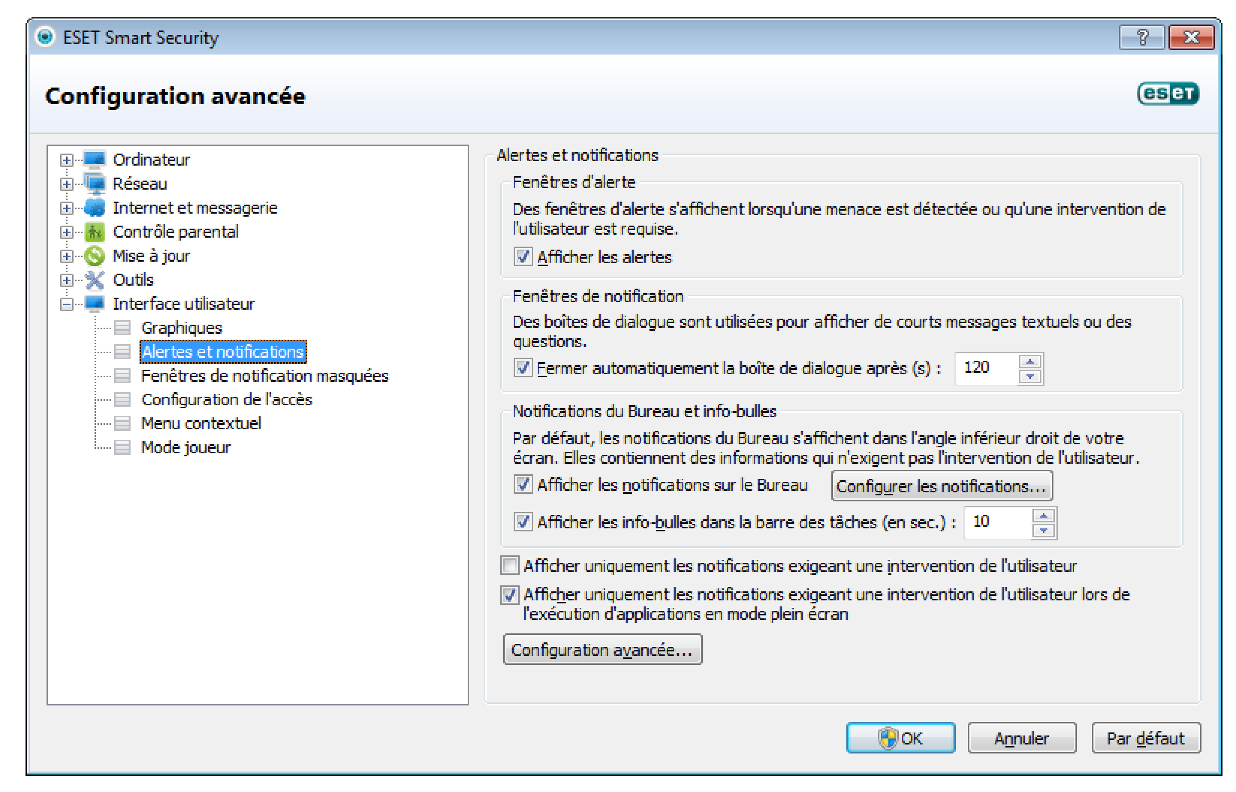
La section **Alertes et notifications** sous **Interface utilisateur** vous permet de configurer la manière dont ESET Smart Security traite les alertes de menace et les notifications système (par ex. les messages indiquant une mise à jour réussie). Vous pouvez également configurer l'heure d'affichage et le niveau de transparence des notifications dans la barre d'état système (ne s'applique qu'aux systèmes prenant en charge ces notifications).

La première option est **Afficher les alertes**. Lorsqu'elle est désactivée, aucune fenêtre d'alerte ne s'affiche, ce qui ne convient qu'à un nombre limité de situations particulières. Nous recommandons à la majorité des utilisateurs de conserver l'option par défaut (activée).

Pour fermer automatiquement les fenêtres d'alerte après un certain délai, sélectionnez l'option **Fermer automatiquement la boîte de dialogue après (sec.)**. Si les fenêtres d'alerte ne sont pas fermées manuellement, le système les ferme automatiquement une fois le laps de temps écoulé.

Les notifications sur le bureau et les infobulles sont fournies à titre d'information uniquement et ne permettent ni n'exigent aucune interaction avec l'utilisateur. Elles s'affichent dans la partie système de la barre d'état, dans l'angle inférieur droit de l'écran. Pour activer l'affichage des notifications sur le bureau, activez l'option **Afficher les notifications sur le bureau**. D'autres options détaillées (la durée d'affichage des notifications et la transparence de la fenêtre) peuvent être modifiées en cliquant sur le bouton **Configurer les notifications...** Pour prévisualiser le comportement des notifications, cliquez sur le bouton **Aperçu**.

Pour configurer la durée d'affichage des infobulles, entrez la durée désirée dans le champ de l'option **Afficher les infobulles dans la barre des tâches (en sec.)**.



L'option **Afficher uniquement les notifications exigeant une intervention de l'utilisateur** vous permet d'activer/de désactiver l'affichage des alertes et des notifications qui n'exigent aucune interaction de l'utilisateur. Sélectionnez **Afficher uniquement les notifications exigeant une intervention de l'utilisateur lors de l'exécution d'applications en mode plein écran** pour supprimer toutes les notifications non interactives.

Cliquez sur **Configuration avancée...** pour accéder aux options supplémentaires de configuration **Alertes et notification**.

4.7.2.1 Configuration avancée

Dans le menu déroulant **Verbosité minimale des événements à afficher**, vous pouvez sélectionner le niveau de gravité de démarrage des alertes et notifications à afficher.

- **Diagnostic** - Consigne toutes les informations nécessaires au réglage du programme et de toutes les entrées ci-dessus.
- **Entrées informatives** - Enregistre tous les messages d'information, y compris les messages de mises à jour réussies et toutes les entrées ci-dessus.
- **Avertissements** - Enregistre les erreurs critiques, les erreurs et les messages d'avertissement.
- **Erreurs** - Consigne les erreurs du type *« Erreur de téléchargement du fichier »* et erreurs critiques.
- **Critique** - Répertorie toutes les erreurs critiques (erreur de démarrage de la protection antivirus, pare-feu personnel, etc...).

La dernière fonctionnalité de cette section permet de configurer la destination des notifications dans un environnement multi-utilisateur. Le champ **Sur les systèmes multi-utilisateurs, afficher les notifications sur l'écran de l'utilisateur suivant** indique l'utilisateur qui recevra les notifications système et autres notifications lorsque le système autorise la connexion simultanée de plusieurs utilisateurs. Normalement, il doit s'agir de l'administrateur système ou de l'administrateur réseau. Cette option est particulièrement utile pour les serveurs Terminal Server, à condition que toutes les notifications système soient envoyées à l'administrateur.

4.7.3 Fenêtres de notification masquées

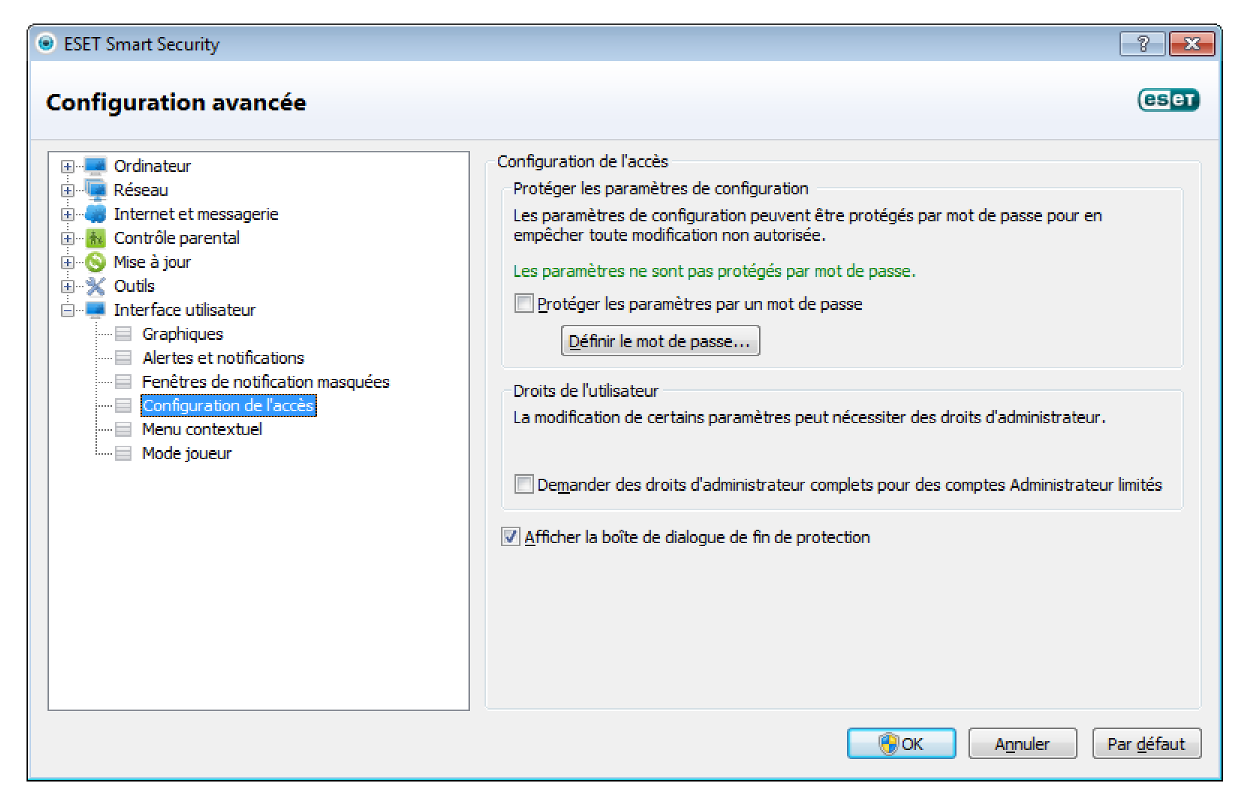
Si l'option **Ne plus afficher ce message** a été sélectionnée pour une fenêtre de notification (alerte) affichée précédemment, cette fenêtre figure dans la liste des fenêtres de notification masquées. Les actions désormais exécutées automatiquement s'affichent dans la colonne intitulée **Confirmer**.

Afficher - Affiche un aperçu des fenêtres de notification non affichées pour lesquelles une action automatique est configurée.

Supprimer - Supprime les éléments de la liste **Boîtes de message masquées**. Toutes les fenêtres de notification supprimées de la liste s'affichent de nouveau.

4.7.4 Configuration de l'accès

Il est essentiel qu'ESET Smart Security soit correctement configuré pour garantir une sécurité maximale du système. Tout changement inapproprié peut entraîner la perte de données importantes. Cette option se trouve dans le sous-menu **Configuration de l'accès**, sous **Interface utilisateur** dans la configuration avancée complète. Pour éviter des modifications non autorisées, les paramètres de la configuration d'ESET Smart Security peuvent être protégés par mot de passe.



Protection des paramètres par mot de passe - Verrouille ou déverrouille les paramètres de configuration du programme. Activez ou désactivez la case à cocher pour ouvrir la fenêtre de configuration du mot de passe.

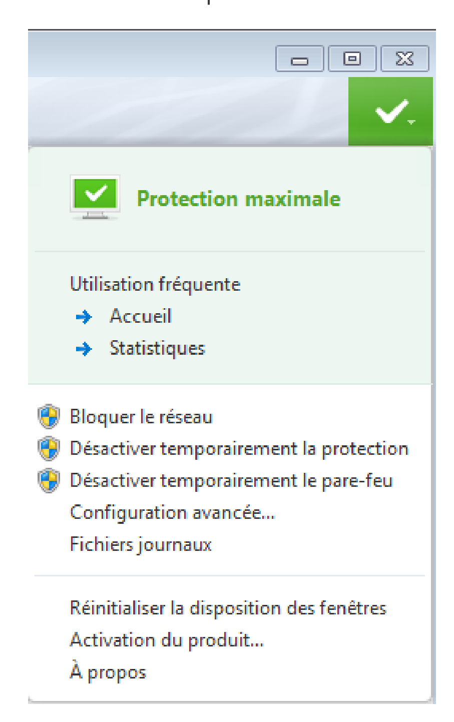
Pour définir ou modifier un mot de passe visant à protéger les paramètres de configuration, cliquez sur **Définir le mot de passe...**

Demander des droits d'administrateur complets pour des comptes Administrateur limités - Sélectionnez cette option pour inviter l'utilisateur actuel (s'il ne possède pas les autorisations d'administrateur) à saisir un nom d'utilisateur et un mot de passe d'administrateur lors de la modification de certains paramètres du système (semblable au contrôle UAC dans Windows Vista). Les modifications comprennent la désactivation des modules de protection ou l'arrêt du pare-feu.

Afficher la boîte de dialogue de fin de protection - Si cette option est sélectionnée, un message apparaît lorsque la protection est temporairement désactivée à partir du menu des programmes ou via la section **ESET Smart Security** > **Configuration**. Le menu déroulant **Intervalle** de la fenêtre **Désactiver temporairement la protection** représente la période pendant laquelle toutes les protections sont désactivées.

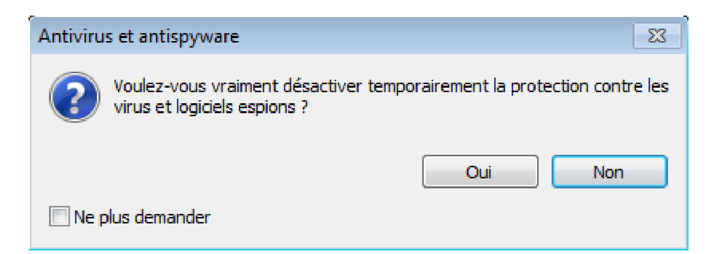
4.7.5 Menu du programme

Certaines des options et fonctionnalités principales se trouvent dans le menu principal du programme.

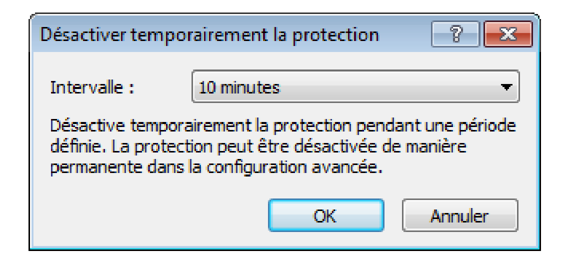


Utilisation fréquente - Affiche les parties les plus utilisées de ESET Smart Security. Vous pouvez y accéder rapidement depuis le menu du programme.

Désactiver temporairement la protection - Affiche la boîte de dialogue de confirmation qui désactive la protection antivirus et antispyware ; cette dernière protège des attaques malveillantes en contrôlant les fichiers, l'Internet et les communications par e-mail. Cochez la case **Ne plus demander** pour éviter de recevoir ce message.



Le menu déroulant **Intervalle** indique la durée pendant laquelle la protection antivirus et antispyware est désactivée.



Bloquer le réseau - Le pare-feu personnel bloque tout le trafic réseau et Internet entrant et sortant.

Désactiver temporairement le pare-feu - Le pare-feu passe en mode inactif. Reportez-vous au chapitre Intégration système du pare-feu personnel pour plus d'informations.

Configuration avancée... - Sélectionnez cette option pour afficher la **Configuration avancée** complète. Vous pouvez également l'ouvrir en appuyant par exemple sur la touche F5 ou en sélectionnant **Configuration** > **Accéder à la configuration avancée...**

Fichiers journaux - Les fichiers journaux contiennent tous les événements importants qui se sont produits et fournissent un aperçu des menaces détectées.

Réinitialiser la disposition des fenêtres - Réinitialise la fenêtre ESET Smart Security sur sa taille et sa position par défaut.

Activation du produit... - Sélectionnez cette option pour activer le produit de sécurité ESET.

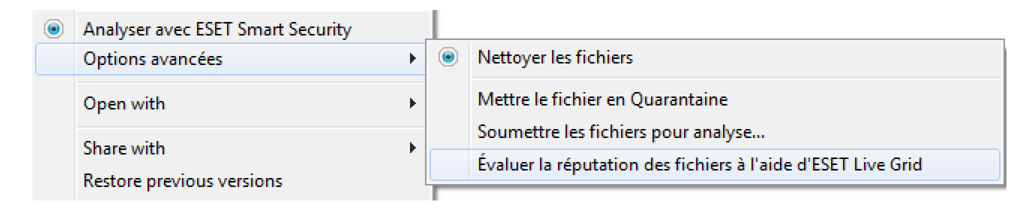
À propos - Les informations système fournissent des détails sur la version installée d'ESET Smart Security et sur les modules installés. Vous y trouverez aussi la date d'expiration de la licence. Dans la partie inférieure figurent des informations sur le système d'exploitation et les ressources du système.

4.7.6 Menu contextuel

Le menu contextuel est le menu qui s'affiche lorsque vous cliquez sur un élément avec le bouton droit de la souris. Le menu répertorie toutes les options disponibles applicables à l'objet.

Il est possible d'intégrer les options ESET Smart Security dans le menu contextuel. La configuration avancée complète contient des options de configuration plus détaillées pour cette fonctionnalité sous **Interface utilisateur** > **Menu contextuel**.

Intégrer dans le menu contextuel - Intègre les options ESET Smart Security dans le menu contextuel.



Les options suivantes sont disponibles dans le menu contextuel **Type de menu** :

- **Complet (analyser d'abord)** - Active toutes les options de menu contextuel ; le menu principal affiche l'option **Analyser avecESET Smart Security**.
- **Complet (nettoyer d'abord)** - Active toutes les options de menu contextuel ; le menu principal affiche l'option **Nettoyer avecESET Smart Security**.
- **Analyse uniquement** - Seule l'option **Analyser avec ESET Smart Security** s'affiche dans le menu contextuel.
- **Nettoyage uniquement** - Seule l'option **Nettoyer avec ESET Smart Security** s'affiche dans le menu contextuel.

4.7.7 Mode joueur

Mode joueur est une fonctionnalité destinée aux utilisateurs qui ont besoin de ne pas être interrompus lors de l'utilisation de leur logiciel. Ils ne souhaitent pas être dérangés par des fenêtres contextuelles et veulent réduire les contraintes sur l'UC. Mode joueur peut également être utilisé au cours de présentations qui ne peuvent pas être interrompues par l'activité antivirus. Lorsque cette fonctionnalité est activée, toutes les fenêtres contextuelles sont désactivées et l'activité du planificateur est complètement arrêtée. La protection du système continue à fonctionner en arrière-plan, mais n'exige aucune interaction de la part de l'utilisateur.

Vous pouvez activer ou désactiver Mode joueur dans la fenêtre principale du programme, en cliquant sur **configuration** > **Ordinateur**, puis sur **Activer** sous **Mode joueur** ; ou vous pouvez activer le Mode joueur dans la configuration avancée complète (F5) en développant **Interface utilisateur**, en cliquant sur **Mode joueur** et en sélectionnant la case à cocher située en regard de **Activer le mode joueur**. L'activation de Mode joueur présentant un risque potentiel pour la sécurité, l'icône d'état de la protection située dans la barre des tâches devient orange et affiche un symbole d'avertissement. Ce symbole apparaît également dans la fenêtre principale du programme, où Mode joueur activé en orange.

Lorsque vous cochez la case **Activer Mode joueur lors de l'exécution automatique d'applications en mode plein écran**, le Mode joueur démarre lorsque vous lancez une application en plein écran et s'arrête lorsque vous quittez l'application. Cette option est particulièrement utile, car elle permet de lancer Mode joueur directement après le démarrage d'un jeu, l'ouverture en plein écran d'une application ou le démarrage d'une présentation.

Vous pouvez également sélectionner la case à cocher **Désactiver Mode joueur automatiquement après X minutes** pour définir la durée (la valeur par défaut est de 1 minute). Cette option n'est utile que si vous souhaitez utiliser Mode joueur pendant un temps défini, puis l'arrêter automatiquement.

REMARQUE : Si le pare-feu personnel est en mode interactif et que Mode joueur est activé, vous pouvez avoir des difficultés à vous connecter à Internet Cela peut être problématique si vous démarrez un jeu qui se connecte à Internet. En temps normal, vous recevez une demande de confirmation de cette action (si aucune règle de communication ni exception n'a été définie), mais l'interaction utilisateur est désactivée en Mode joueur. La solution consiste à définir une règle de communication pour chaque application pouvant entrer en conflit avec ce comportement. Il est également possible d'utiliser un autre mode de filtrage dans le pare-feu personnel. Notez en outre que si Mode joueur est activé, et que vous accédez à une page Web ou à une application qui peut présenter une menace, la page est bloquée, mais vous ne recevez aucune explication ni avertissement, puisque l'interaction utilisateur est désactivée.

5. Utilisateur chevronné

5.1 Configuration du serveur proxy

Dans les grands réseaux locaux, la connexion de votre ordinateur à Internet peut s'effectuer par l'intermédiaire d'un serveur proxy. Si c'est le cas, les paramètres suivants doivent être définis. Dans le cas contraire, le programme ne pourra pas se mettre à jour automatiquement. Dans ESET Smart Security, il est possible de configurer le serveur proxy à partir de deux sections de la configuration avancée complète.

Tout d'abord, les paramètres de serveur proxy peuvent être configurés dans **Configuration avancée**, depuis **Outils** > **Serveur proxy**. La spécification du serveur proxy à ce niveau définit les paramètres de serveur proxy globaux pour l'intégralité d'ESET Smart Security. Les paramètres définis ici seront utilisés par tous les modules exigeant une connexion à Internet.

Pour spécifier des paramètres de serveur proxy à ce niveau, cochez la case **Utiliser un serveur proxy**, puis entrez l'adresse du serveur proxy dans le champ **Serveur proxy**, ainsi que le numéro de **port** de ce serveur proxy.

Si la communication avec le serveur proxy exige une authentification, cochez la case **Le serveur proxy nécessite une authentification** et entrez un **nom d'utilisateur** et un **mot de passe** valides dans les champs correspondants. Cliquez sur le bouton **Détecter le serveur proxy** pour détecter automatiquement et insérer les paramètres du serveur proxy. Les paramètres indiqués dans Internet Explorer sont copiés.

REMARQUE : cette fonctionnalité ne récupère pas les données d'authentification (nom d'utilisateur et mot de passe) ; vous devez donc les fournir.

Les paramètres de serveur proxy peuvent également être établis dans la configuration avancée de la mise à jour (section **Mettre à jour** de la **Configuration avancée** complète). Ce paramètre s'applique au profil de mise à jour donné et est recommandé pour les ordinateurs portables, car il permet de recevoir les mises à jour de la base des signatures de virus depuis différents emplacements. Pour plus d'informations sur ce paramètre, consultez la section Configuration avancée des mises à jour.

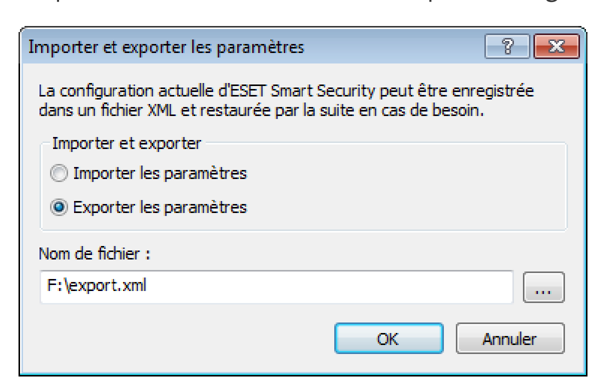
5.2 Importer et exporter les paramètres

L'importation et l'exportation des configurations d'ESET Smart Security sont disponibles dans **Configuration**.

L'importation et l'exportation utilisent le type de fichier *.xml*. Ces opérations sont utiles si vous devez sauvegarder la configuration actuelle d'ESET Smart Security pour l'utiliser ultérieurement. L'option Exporter les paramètres est également pratique pour les utilisateurs qui souhaitent utiliser leur configuration ESET Smart Security préférée sur plusieurs systèmes. Il leur suffit d'importer un fichier *.xml* pour transférer les paramètres souhaités.

L'importation d'une configuration est très facile. Dans la fenêtre principale du programme, cliquez sur **Configuration** > **Importer et exporter les paramètres...**, puis sélectionnez l'option **Importer les paramètres**. Saisissez le chemin d'accès au fichier de configuration ou cliquez sur le bouton **...** pour accéder au fichier de configuration à importer.

La procédure d'exportation d'une configuration est très semblable. Dans la fenêtre principale du programme, cliquez sur **Configuration** > **Importer et exporter les paramètres...** Sélectionnez l'option **Exporter les paramètres** et saisissez le **nom de fichier** du fichier de configuration (par exemple *export.xml*). Utilisez le navigateur pour sélectionner un emplacement de votre ordinateur pour enregistrer le fichier de configuration.



5.3 Raccourcis clavier

Voici les raccourcis clavier disponibles dans ESET Smart Security :

Ctrl+G	désactive l'interface utilisateur dans le produit
Ctrl+I	ouvre la page ESET SysInspector
Ctrl+L	ouvre la page des fichiers journaux
Ctrl+S	ouvre la page du planificateur
Ctrl+Q	ouvre la page de quarantaine
Ctrl+U	ouvre une boîte de dialogue permettant d'indiquer le nom d'utilisateur et le mot de passe
Ctrl+R	réinitialise la taille et la position par défaut de la fenêtre à l'écran

Pour simplifier la navigation dans le produit de sécurité ESET, vous pouvez utiliser les raccourcis clavier suivants :

F1	ouvre les pages d'aide
F5	ouvre la boîte de dialogue Configuration avancée
Haut/Bas	navigation dans les différents composants du produit
*	développe le nœud de l'arborescence Configuration avancée
-	réduit le nœud de l'arborescence Configuration avancée
TAB	déplace le curseur dans une fenêtre
Échap	ferme la boîte de dialogue active

5.4 Ligne de commande

Le module antivirus d'ESET Smart Security peut être lancé depuis la ligne de commande, manuellement (avec la commande « ecls ») ou au moyen d'un fichier de traitement par lots (« bat »). Module d'interface à ligne de commande ESET :

```
ecls [OPTIONS..] FILES..
```

Les paramètres suivants peuvent être utilisés lors de l'exécution de l'analyseur à la demande, à partir de la ligne de commande :

Options

/base-dir=FOLDER	charger les modules depuis le DOSSIER
/quar-dir=FOLDER	DOSSIER de quarantaine
/exclude=MASK	exclure les fichiers correspondant à MASQUE de l'analyse
/subdir	analyser les sous-dossiers (valeur par défaut)
/no-subdir	ne pas analyser les sous-dossiers
/max-subdir-level=LEVEL	sous-niveau maximal de sous-dossiers dans les dossiers à analyser
/symlink	suivre les liens symboliques (valeur par défaut)
/no-symlink	ignorer les liens symboliques
/ads	analyser ADS (valeur par défaut)
/no-ads	ne pas analyser ADS
/log-file=FILE	journaliser les résultats dans un FICHIER
/log-rewrite	écraser le fichier de résultats (valeur par défaut - ajouter)
/log-console	journaliser les résultats sur la console (valeur par défaut)
/no-log-console	ne pas journaliser les résultats sur la console
/log-all	journaliser également les fichiers nettoyés
/no-log-all	ne pas journaliser les fichiers nettoyés (valeur par défaut)
/aind	afficher l'indicateur d'activité
/auto	analyser et nettoyer automatiquement tous les disques locaux

Options de l'analyseur

/files	analyser les fichiers (valeur par défaut)
/no-files	ne pas analyser les fichiers
/memory	analyser la mémoire
/boots	analyser les secteurs d'amorçage
/no-boots	ne pas analyser les secteurs d'amorçage (valeur par défaut)
/arch	analyser les archives (valeur par défaut)
/no-arch	ne pas analyser les archives

/max-obj-size=SIZE	analyser uniquement les fichiers plus petits que TAILLE Mo (valeur par défaut 0 = illimité)
/max-arch-level=LEVEL	sous-niveau maximal d'archives à analyser dans les archives (archives imbriquées)
/scan-timeout=LIMIT	analyser les archives pendant un maximum de LIMITE secondes
/max-arch-size=SIZE	n'analyser les fichiers contenus dans une archive que s'ils sont plus petits que TAILLE (valeur par défaut 0 = illimité)
/max-sfx-size=SIZE	n'analyser les fichiers d'une archive auto-extractible que s'ils sont plus petits que TAILLE Mo (valeur par défaut 0 = illimité)
/mail	analyser les fichiers des courriers électroniques (valeur par défaut)
/no-mail	ne pas analyser les fichiers des courriers électroniques
/mailbox	analyser les boîtes aux lettres (valeur par défaut)
/no-mailbox	ne pas analyser les boîtes aux lettres
/sfx	analyser les archives auto-extractibles (valeur par défaut)
/no-sfx	ne pas analyser les archives auto-extractibles
/rtp	analyser les fichiers exécutables compressés par un compresseur d'exécutables (valeur par défaut)
/no-rtp	ne pas analyser les fichiers exécutables compressés
/adware	rechercher les adware/spyware/riskware (valeur par défaut)
/no-adware	ne pas rechercher les adware/spyware/riskware
/unsafe	rechercher les applications potentiellement dangereuses
/no-unsafe	ne pas rechercher les applications potentiellement dangereuses (valeur par défaut)
/unwanted	rechercher les applications potentiellement indésirables
/no-unwanted	ne pas rechercher les applications potentiellement indésirables (valeur par défaut)
/pattern	utiliser les signatures (valeur par défaut)
/no-pattern	ne pas utiliser les signatures
/heur	activer l'heuristique (valeur par défaut)
/no-heur	désactiver l'heuristique
/adv-heur	activer l'heuristique avancée (valeur par défaut)
/no-adv-heur	désactiver l'heuristique avancée
/ext=EXTENSIONS	analyser uniquement les EXTENSIONS délimitées par deux-points
/ext-exclude=EXTENSIONS	exclure de l'analyse les EXTENSIONS délimitées par deux-points
/clean-mode=MODE	utiliser le MODE de nettoyage pour les objets infectés. Les options disponibles sont les suivantes : aucun nettoyage, nettoyage standard (valeur par défaut), nettoyage strict, nettoyage rigoureux, suppression
/quarantine	copier les fichiers infectés (si nettoyés) vers Quarantaine (complète l'action effectuée lors du nettoyage)
/no-quarantine	ne pas copier les fichiers infectés vers Quarantaine

Options générales

/help	afficher l'aide et quitter
/version	afficher les informations de version et quitter
/preserve-time	conserver la date et l'heure du dernier accès

Codes de sortie

0	aucune menace détectée
1	menace détectée et nettoyée
10	certains fichiers n'ont pas pu être analysés (peuvent être des menaces)
50	menace détectée
100	erreur

REMARQUE : un code sortie supérieur à 100 signale un fichier non analysé qui est potentiellement infecté.

5.5 ESET SysInspector

5.5.1 Introduction à ESET SysInspector

ESET SysInspector est une application qui inspecte votre ordinateur en profondeur et qui affiche en détail toutes les données obtenues. Des informations telles que les pilotes et applications installés, les connexions réseau ou les entrées de registre importantes peuvent vous aider à élucider un comportement suspect du système, qu'il soit dû à une incompatibilité logicielle ou matérielle, ou à une infection par logiciel malveillant.

Vous pouvez accéder à ESET SysInspector de deux manières : depuis la version intégrée dans les solutions ESET Security ou en téléchargeant gratuitement la version autonome (SysInspector.exe) depuis le site Internet d'ESET. Les deux versions sont identiques en matière de fonctionnalités et disposent des mêmes contrôles de programme. La seule différence réside dans la façon dont les résultats sont gérés. Les versions téléchargées et intégrées vous permettent d'exporter des instantanés du système dans un fichier *.xml* et de les enregistrer sur le disque. Toutefois, la version intégrée vous permet également de stocker les instantanés du système directement dans **Outils** > **ESET SysInspector** (à l'exception de ESET Remote Administrator). Pour plus d'informations, reportez-vous à la section ESET SysInspector comme composant de ESET Smart Security.

Veuillez patienter pendant qu'ESET SysInspector analyse votre ordinateur. L'analyse peut prendre entre 10 secondes et quelques minutes, en fonction de la configuration de votre matériel, du système d'exploitation et du nombre d'applications installées sur votre ordinateur.

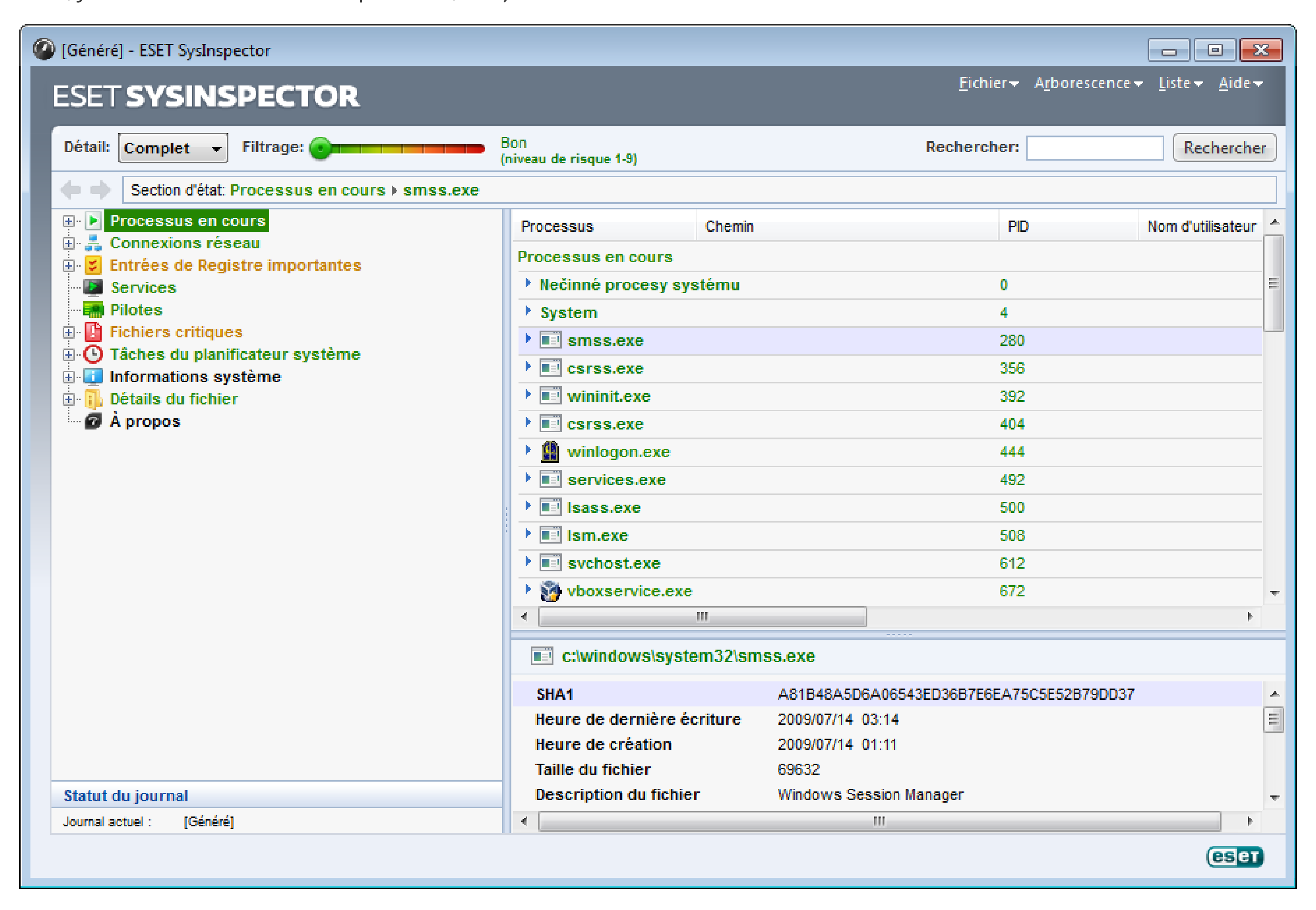
5.5.1.1 Démarrage d'ESET SysInspector

Pour démarrer ESET SysInspector, il suffit de lancer le fichier exécutable *SysInspector.exe* téléchargé depuis le site Web d'ESET. Si vous avez déjà installé une des solutions ESET Security, vous pouvez exécuter ESET SysInspector directement depuis le menu Démarrer (**Programmes** > **ESET** > **ESET Smart Security**).

Patientez pendant que l'application vérifie le système. Cette opération peut prendre plusieurs minutes, en fonction du matériel et des données à recueillir.

5.5.2 Interface utilisateur et utilisation de l'application

Pour des raisons de clarté, la fenêtre principale est divisée en quatre principales sections : la section des Contrôles du programme en haut, la fenêtre Navigation à gauche, la fenêtre Description à droite au centre et la fenêtre Détails à droite au bas. La section État du journal énumère les paramètres de base d'un journal (utilisation des filtres, type de filtre, journal résultat d'une comparaison, etc.).



5.5.2.1 Contrôles du programme

Cette section contient la description de tous les contrôles du programme disponible dans ESET SysInspector.

Fichier

En cliquant sur l'option **Fichier**, vous pouvez enregistrer l'état actuel du système en vue d'une enquête ultérieure ou ouvrir un journal déjà enregistré. Pour la publication, il est conseillé de créer un journal **approprié pour envoi**. Sous cette forme, le journal omet les informations sensibles (nom d'utilisateur, nom d'ordinateur, nom de domaine, privilèges actuels de l'utilisateur, variables d'environnement, etc.).

REMARQUE : vous pouvez ouvrir des rapports enregistrés ESET SysInspector en les faisant glisser et en les déposant sur la fenêtre principale.

Arborescence

Permet de développer ou de réduire tous les nœuds et d'exporter les sections sélectionnées dans le script de service.

Liste

Contient des fonctions qui simplifient la navigation dans le programme, ainsi que d'autres fonctionnalités comme l'obtention d'informations en ligne.

Aide

Contient des informations sur l'application et ses fonctions.

Détails

Ce paramètre conditionne les informations affichées dans la fenêtre principale, ce qui simplifie leur utilisation. En mode de base, vous avez accès aux informations utilisées pour trouver les solutions aux problèmes communs dans votre système. En mode Moyen, le programme affiche moins de détails. En mode Complet, ESET SysInspector affiche toutes les informations nécessaires pour résoudre des problèmes très précis.

Filtrage des éléments

Le filtrage des éléments est particulièrement adapté à la recherche de fichiers suspects ou d'entrées de registre dans le système. En déplaçant le curseur, vous pouvez filtrer les éléments en fonction de leur niveau de risque. Quand le curseur est en position maximale vers la gauche (niveau de risque 1), tous les éléments sont affichés. En déplaçant le curseur vers la droite, l'application filtre tous les éléments dont le risque est inférieur au niveau de risque actuel et affiche uniquement les éléments qui sont plus suspects que le niveau affiché. Si le curseur est en position maximale à droite, le programme affiche uniquement les éléments nuisibles connus.

Tous les éléments portant le niveau de risque 6 à 9 peuvent poser un risque pour la sécurité. Si vous n'utilisez pas de solution de sécurité d'ESET, nous vous conseillons d'analyser votre système à l'aide d'ESET Online Scanner si ESET SysInspector a détecté un élément de ce genre. ESET Online Scanner est un service gratuit.

REMARQUE : le niveau de risque d'un élément peut être rapidement déterminé grâce à la couleur que prend le curseur pour indiquer le niveau de risque.

Rechercher

La fonction de recherche permet de trouver rapidement un élément sur la base de son nom ou d'une partie de son nom. Les résultats de la recherche sont affichés dans la fenêtre Description.

Retour

En cliquant sur la flèche arrière ou avant, vous pouvez revenir aux informations affichées précédemment dans la fenêtre Description. Vous pouvez utiliser la touche de retour arrière et la barre d'espace au lieu de cliquer sur les flèches arrière ou avant.

Section d'état

Affiche le nœud actuel dans la fenêtre Navigation.

Important : les éléments surlignés en rouge sont inconnus et c'est la raison pour laquelle l'application les marque comme potentiellement dangereux. Si un élément est rouge, cela ne signifie pas automatiquement que vous pouvez supprimer le fichier. Avant de le supprimer, assurez-vous que les fichiers sont bel et bien dangereux ou qu'ils ne sont pas nécessaires.

5.5.2.2 Navigation dans ESET SysInspector

ESET SysInspector répartit divers types d'informations en plusieurs sections principales appelées nœuds. Le cas échéant, vous pouvez obtenir des détails complémentaires en développant chaque nœud afin d'afficher les sous-nœuds. Pour développer ou réduire un nœud, il suffit de double-cliquer sur son nom ou de cliquer sur ⊞ ou sur ⊟ en regard du nom du nœud. Quand vous parcourez l'arborescence des nœuds et des sous-nœuds dans la fenêtre de navigation, vous pouvez voir différents détails pour chaque nœud dans la fenêtre Description. Si vous parcourez les éléments de la fenêtre Description, des détails supplémentaires pour chaque élément peuvent être affichés dans la fenêtre Détails.

Voici les descriptions des principaux nœuds de la fenêtre Navigation et des informations qui s'y rapportent dans les fenêtres Description et Détails.

Processus en cours

Ce nœud comprend les informations sur les applications et les processus en cours d'exécution au moment de la création du journal. La fenêtre Détails comprend des détails complémentaires pour chaque processus tels que les bibliothèques dynamiques utilisées par les processus et leur emplacement dans le système, le nom de l'éditeur de l'application et le niveau de risque du fichier.

La fenêtre Détails contient des informations complémentaires sur les éléments sélectionnés dans la fenêtre Description telles que la taille du fichier ou son hachage.

REMARQUE : un système d'exploitation contient plusieurs noyaux importants qui fonctionnent en permanence et qui assurent des fonctions élémentaires et vitales pour d'autres applications utilisateur. Dans certains cas, ces processus sont repris dans l'outil ESET SysInspector avec un chemin d'accès au fichier commençant par \??\. Ces symboles

garantissent l'optimisation préalable au lancement de ces processus ; ils ne présentent aucun danger pour le système.

Connexions réseau

La fenêtre Description contient la liste des processus et des applications qui communiquent via le réseau à l'aide du protocole sélectionné dans la fenêtre navigation (TCP ou UDP), ainsi que l'adresse distante à laquelle l'application est connectée. Vous pouvez également vérifier les adresses IP des serveurs DNS.

La fenêtre Détails contient des informations complémentaires sur les éléments sélectionnés dans la fenêtre Description telles que la taille du fichier ou son hachage.

Entrées de registre importantes

Contient la liste des entrées de registre sélectionnées qui sont souvent liées à des problèmes système. Il s'agit des entrées qui indiquent les applications de démarrage, les objets d'application d'assistance du navigateur, etc.

La fenêtre Description peut indiquer les fichiers en rapport avec les entrées de registre particulières. Vous pouvez voir des détails complémentaires dans la fenêtre Détails.

Services

La fenêtre Description contient la liste des fichiers enregistrés en tant que services Windows. Vous pouvez consulter la manière dont le service doit démarrer avec des détails spécifiques sur le fichier dans la fenêtre Détails.

Pilotes

Liste des pilotes installés sur le système.

Fichiers critiques

La fenêtre Description affiche le contenu des fichiers critiques liés au système d'exploitation Microsoft Windows.

Tâches du planificateur système

Contient une liste des tâches déclenchées par le planificateur de tâches Windows à une heure/un intervalle défini.

Informations système

Contient des informations détaillées sur le matériel et le logiciel, ainsi que des informations sur les variables d'environnement, les droits d'utilisateur et les journaux d'événements système définis.

Détails du fichier

Liste des fichiers système importants et des fichiers du dossier Program Files. Des informations complémentaires spécifiques sur les fichiers sont disponibles dans les fenêtres Description et Détails.

À propos de

Informations relatives à la version d'ESET SysInspector et liste des modules du programme.

5.5.2.2.1 Raccourcis clavier

Voici les raccourcis clavier disponibles dans ESET SysInspector :

Fichier

Ctrl+O	ouvre un journal existant
Ctrl+S	enregistre les journaux créés

Générer

Ctrl+G	génère un instantané standard du statut de l'ordinateur
Ctrl+H	génère un instantané du statut de l'ordinateur qui est susceptible de contenir des informations sensibles

Filtrage des éléments

1, O	affiche les éléments de niveau de risque 1 à 9 (acceptable)
2	affiche les éléments de niveau de risque 2 à 9 (acceptable)
3	affiche les éléments de niveau de risque 3 à 9 (acceptable)
4, U	affiche les éléments de niveau de risque 4 à 9 (inconnu)
5	affiche les éléments de niveau de risque 5 à 9 (inconnu)

6	affiche les éléments de niveau de risque 6 à 9 (inconnu)
7, B	affiche les éléments de niveau de risque 7 à 9 (risqué)
8	affiche les éléments de niveau de risque 8 à 9 (risqué)
9	affiche les éléments de niveau de risque 9 (risqué)
-	diminue le niveau de risque
+	augmente le niveau de risque
Ctrl+9	mode de filtrage, niveau égal ou supérieur
Ctrl+O	mode de filtrage, niveau égal uniquement

Afficher

Ctrl+5	afficher par éditeur, tous les éditeurs
Ctrl+6	afficher par éditeur, uniquement Microsoft
Ctrl+7	afficher par éditeur, tous les autres éditeurs
Ctrl+3	afficher tous les détails
Ctrl+2	afficher les détails de précision moyenne
Ctrl+1	affichage de base
Retour arrière	revient une étape en arrière
Barre d'espace	avance d'une étape
Ctrl+W	développe l'arborescence
Ctrl+Q	réduit l'arborescence

Autres commandes

Ctrl+T	accède à l'emplacement d'origine de l'élément après la sélection dans les résultats de recherche
Ctrl+P	affiche des informations élémentaires sur un élément
Ctrl+A	affiche des informations complètes sur un élément
Ctrl+C	copie l'arborescence de l'élément
Ctrl+X	copie les éléments
Ctrl+B	trouve des informations sur les fichiers sélectionnés sur Internet
Ctrl+L	ouvre le dossier où se trouve le fichier sélectionné.
Ctrl+R	ouvre l'entrée correspondante dans l'éditeur de registre
Ctrl+Z	copie un chemin d'accès à un fichier (si l'élément est lié à un fichier)
Ctrl+F	passe au champ de recherche
Ctrl+D	ferme les résultats de la recherche
Ctrl+E	exécute le script de service

Comparaison

Ctrl+Alt+O	ouvre le journal d'origine/de comparaison
Ctrl+Alt+R	annule la comparaison
Ctrl+Alt+1	affiche tous les éléments
Ctrl+Alt+2	affiche uniquement les éléments ajoutés ; le journal indique les éléments présents dans le journal actuel
Ctrl+Alt+3	affiche uniquement les éléments supprimés ; le journal indique les éléments présents dans le journal précédent
Ctrl+Alt+4	affiche uniquement les éléments remplacés (fichiers inclus)
Ctrl+Alt+5	affiche uniquement les différences entre les journaux
Ctrl+Alt+C	affiche la comparaison
Ctrl+Alt+N	affiche le journal actuel
Ctrl+Alt+P	ouvre le journal précédent

Divers

F1	afficher l'aide
Alt+F4	quitter l'application
Alt+Maj+F4	quitter l'application sans demander
Ctrl+I	statistiques du journal

5.5.2.3 Comparer

La fonctionnalité Comparer permet de comparer deux journaux. Cette fonctionnalité met en évidence les éléments qui ne sont pas communs aux deux journaux. Ce procédé est utile si vous souhaitez assurer le suivi des modifications dans le système. Vous pourrez peut-être ainsi détecter l'activité d'un code malveillant.

Après son lancement, l'application crée un journal qui apparaît dans une nouvelle fenêtre. Accédez au menu **Fichier** > **Enregistrer le journal** pour enregistrer le journal dans un fichier. Les fichiers journaux peuvent être ouverts et consultés ultérieurement. Pour ouvrir un journal existant, utilisez le menu **Fichier** > **Ouvrir le journal**. Dans la fenêtre principale de l'application, ESET SysInspector affiche toujours un journal à la fois.

Le fait de comparer deux journaux permet d'afficher le journal actif et un journal enregistré dans un fichier. Pour comparer des journaux, choisissez l'option **Fichier** > **Comparer les journaux**, puis choisissez **Sélectionner un fichier**. Le journal sélectionné est comparé au journal actif dans les fenêtres principales de l'application. Le journal résultant, appelé journal des comparaisons, affiche uniquement les différences entre les deux journaux.

REMARQUE : si vous comparez deux fichiers journaux, choisissez **Fichier** > **Enregistrer le journal** et enregistrez-le dans un fichier ZIP. Les deux fichiers sont enregistrés. Si vous ouvrez ce fichier ultérieurement, les journaux qu'il contient seront comparés automatiquement.

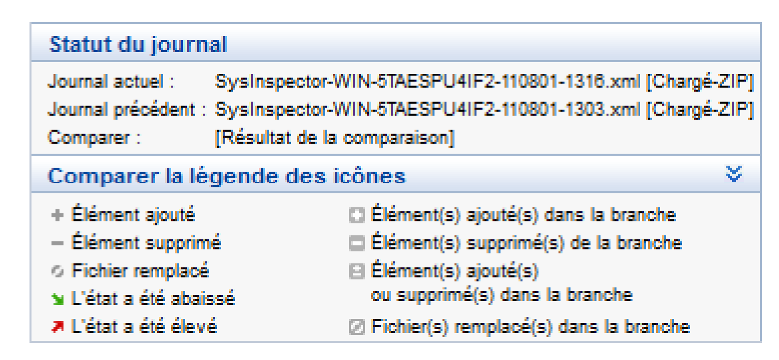
En regard des éléments affichés, ESET SysInspector ajoute des symboles qui identifient les différences entre les journaux comparés.

Les éléments marqués par - se trouvent uniquement dans le journal actif et sont absents du journal de comparaison ouvert. Les éléments marqués par + se trouvent uniquement dans le journal ouvert et ne figurent pas dans le journal actif.

Description de tous les symboles qui peuvent être affichés à côté des éléments :

- + nouvelle valeur, absente du journal précédent.
- cette section de l'arborescence contient de nouvelles valeurs.
- - valeur supprimée, présente uniquement dans le journal précédent.
- cette section de l'arborescence contient des valeurs supprimées.
- valeur/fichier modifié.
- cette section de l'arborescence contient des valeurs/fichiers modifiés.
- le niveau de risque a diminué/était supérieur dans le journal précédent.
- le niveau de risque a augmenté/il était inférieur dans le journal précédent.

La section d'explication affichée dans le coin inférieur gauche décrit tous les symboles et affiche le nom des journaux comparés.



Les journaux de comparaison peuvent être enregistrés dans un fichier et ouverts ultérieurement :

Exemple

Créez un journal reprenant les informations d'origine du système et enregistrez-le dans un fichier appelé précédent.xml. Après avoir modifié le système, ouvrez ESET SysInspector pour qu'il crée un nouveau journal. Enregistrez ce journal sous le nom *actuel.xml*.

Pour voir les différences entre ces deux journaux, utilisez l'option **Fichier** > **Comparer les journaux**. Le programme crée un journal de comparaison qui indique les différences entre les journaux.

Un résultat identique peut être obtenu si vous utilisez l'option de ligne de commande suivante :

SysIsnpector.exe actuel.xml précédent.xml

5.5.3 Paramètres de la ligne de commande

ESET SysInspector prend en charge la création de rapports via la ligne de commande à l'aide de ces paramètres :

/gen	crée un journal directement depuis la ligne de commande sans exécuter l'interface utilisateur.
/privacy	crée un journal qui exclut les informations sensibles.
/zip	stocke le journal obtenu directement sur le disque dans un fichier compressé.
/silent	supprime l'affichage de la barre de progression de la création du journal.
/help, /?	affiche des informations sur les paramètres de la ligne de commande.

Exemples

Pour charger un journal en particulier directement dans le navigateur, saisissez : *SysInspector.exe "c:\clientlog.xml"*
Pour créer un journal à l'emplacement actuel, saisissez : *SysInspector.exe /gen*
Pour créer un journal dans un dossier en particulier, saisissez : *SysInspector.exe /gen="c:\dossier\"*
Pour créer un journal dans un fichier/dossier en particulier, saisissez : *SysInspector.exe /gen="c:\dossier\monnouveaujournal.xml"*
Pour créer un journal qui exclut les informations sensibles directement dans un fichier compressé, saisissez : *SysInspector.exe /gen="c:\monnouveaujournal.zip" /privacy /zip*
Pour comparer deux journaux, utilisez : *SysInspector.exe "actuel.xml" "original.xml"*

REMARQUE : si le nom du fichier/dossier contient un espace, saisissez-le entre guillemets.

5.5.4 Script de service

Le script de service supprime très facilement les objets indésirables du système et offre une aide aux clients qui utilisent ESET SysInspector.

Le script de service permet à l'utilisateur d'exporter l'ensemble du journal ESET SysInspector ou certaines parties sélectionnées. Après l'exportation, vous pouvez marquer les objets non souhaités pour la suppression. Vous pouvez ensuite exécuter le journal modifié pour supprimer les objets marqués.

Le script de service convient aux utilisateurs expérimentés qui connaissent les problèmes des systèmes de diagnostic. Des modifications erronées pourraient endommager le système d'exploitation.

Exemple

Si vous pensez que votre ordinateur est infecté par un virus qui n'est pas détecté par votre logiciel antivirus, suivez les instructions ci-après :

- Exécutez ESET SysInspector pour obtenir un nouvel instantané du système.
- Sélectionnez le premier élément de la section à gauche (dans l'arborescence), appuyez sur la touche Maj et maintenez-la enfoncée, puis sélectionnez le dernier élément afin de marquer tous les éléments.
- Cliquez à l'aide du bouton droit sur les objets sélectionnés et choisissez l'option **Exporter les sections sélectionnées dans un script de service** dans le menu contextuel.
- Les objets sélectionnés sont exportés dans un nouveau journal.
- Il s'agit de l'étape la plus importante de toute la procédure : ouvrez le nouveau journal et remplacez l'attribut - par + pour tous les objets que vous souhaitez supprimer. Assurez-vous que vous n'avez sélectionné aucun objet/fichier important pour le système d'exploitation.
- Ouvrez ESET SysInspector, cliquez sur **Fichier** > **Exécuter le script de services** et entrez le chemin d'accès au script.
- Cliquez sur **OK** pour lancer le script.

5.5.4.1 Création d'un script de service

Pour créer un script, cliquez avec le bouton droit de la souris sur n'importe quel élément de l'arborescence de menus (dans le volet de gauche) dans la fenêtre principale de ESET SysInspector. Dans le menu contextuel, choisissez l'option **Exporter toutes les sections dans un script de service** ou **Exporter les sections sélectionnées dans un script de service**.

REMARQUE : il est impossible d'exporter le script de service lorsque deux journaux sont comparés.

5.5.4.2 Structure du script de service

La première ligne de l'en-tête du script reprend des informations sur la version du moteur (ev), la version de l'interface utilisateur graphique (gv) et la version du journal (lv). Ces données permettent d'identifier d'éventuelles modifications dans le fichier .xml qui génère le script et d'éviter toute incohérence durant l'exécution. Cette partie du script ne peut pas être modifiée.

Le reste du fichier est scindé en sections dont les éléments peuvent être modifiés (elles indiquent les éléments qui sont traités par le script). Pour marquer un élément à traiter, remplacez le caractère « - » qui le précède par « + ». Les sections du script sont séparées par une ligne vide. Chaque section possède un numéro et un titre.

01) Running processes (processus en cours)

Cette section contient la liste de tous les processus en cours d'exécution dans le système. Chaque processus est identifié par son chemin UNC, puis par son code de hachage CRC16 entre astérisques (*).

Exemple :

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

Dans cet exemple, un processus, à savoir module32.exe, a été sélectionné (marqué par le caractère « + ») ; le processus s'arrête à l'exécution du script.

02) Loaded modules (modules chargés)

Cette section répertorie la liste des modules système en cours d'utilisation :

Exemple :

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

Dans cet exemple, le module khbekhb.dll a été marqué par un « + ». Quand le script est exécuté, il reconnaît les processus qui utilisent ce module et les arrête.

03) TCP connections (connexions TCP)

Cette section contient des informations sur les connexions TCP existantes.

Exemple :

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

Lorsque le script est exécuté, il localise le propriétaire du socket dans les connexions TCP marquées et arrête le socket, ce qui libère des ressources système.

04) UDP endpoints (points de terminaison UDP)

Cette section contient des informations sur les points de terminaison UDP existants.

Exemple :

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Lorsque le script est exécuté, il isole le propriétaire du socket aux points de terminaison UDP marqués et arrête le socket.

05) DNS server entries (entrées du serveur DNS)

Cette section contient des informations sur la configuration actuelle du serveur DNS.

Exemple :

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Les entrées du serveur DNS marquées sont supprimées à l'exécution du script.

06) Important registry entries (entrées de registre importantes)

Cette section contient des informations relatives aux entrées de registre importantes.

Exemple :

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

Les entrées marquées sont supprimées, réduites à des valeurs de 0 octet ou réinitialisées sur leur valeur par défaut lors de l'exécution du script. L'action à appliquer sur chaque entrée dépend de la catégorie de l'entrée et de la valeur de la clé dans ce registre.

07) Services (services)

Cette section répertorie les services enregistrés dans le système.

Exemple :

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

Les services marqués et les services dépendants sont arrêtés et désinstallés après l'exécution du script.

08) Drivers (pilotes)

Cette section répertorie les pilotes installés.

Exemple :

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Lorsque vous exécutez le script, les pilotes sélectionnés sont arrêtés. Notez que certains pilotes ne se laisseront pas arrêter.

09) Critical files (fichiers critiques)

Cette section contient des informations sur les fichiers essentiels au bon fonctionnement du système d'exploitation.

Exemple :

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Les éléments sélectionnés sont soit supprimés, soit restaurés sur leur valeur d'origine.

5.5.4.3 Exécution des scripts de services

Marquez tous les éléments souhaités, puis enregistrez et fermez le script. Exécutez le script modifié directement depuis la fenêtre principale ESET SysInspector en choisissant l'option **Exécuter le script de services** dans le menu Fichier. Lorsque vous ouvrez un script, le programme affiche le message suivant : **Voulez-vous vraiment exécuter le script de service « %Scriptname% » ??** Une fois que vous avez confirmé votre sélection, un autre avertissement peut apparaître pour vous indiquer que le script de service que vous essayez d'exécuter n'a pas été signé. Cliquez sur **Exécuter** pour lancer le script.

Une boîte de dialogue confirme l'exécution correcte du script.

Si le script n'a pu être traité que partiellement, une boîte de dialogue avec le message suivant apparaît : **Le script de service n'a été exécuté que partiellement. Voulez-vous afficher le rapport d'erreurs ?** Choisissez **Oui** pour afficher un rapport des erreurs complexe qui répertorie les opérations qui n'ont pas été exécutées.

Si le script n'a pas été reconnu, une boîte de dialogue apparaît avec le message suivant : **Le script de service sélectionné n'est pas signé. L'exécution de scripts non signés et inconnus peut endommager gravement les données de votre ordinateur. Voulez-vous vraiment exécuter le script et ses actions ?** Ceci peut être le résultat d'incohérences au sein du script (en-tête ou titre de section endommagé, ligne vide manquante entre les sections, etc.). Vous pouvez soit rouvrir le fichier de script et corriger les erreurs qu'il contient, soit créer un autre script de service.

5.5.5 FAQ

L'exécution d'ESET SysInspector requiert-elle des privilèges d'administrateur ?

Bien qu'ESET SysInspector puisse être exécuté sans privilèges d'administrateur, certaines des informations qu'il recueille peuvent être consultées uniquement via un compte administrateur. Une exécution en tant qu'utilisateur standard ou utilisateur disposant d'un accès restreint entraîne la collecte d'un volume inférieur d'informations sur l'environnement d'exploitation.

ESET SysInspector crée-t-il un fichier journal ?

ESET SysInspector peut créer un fichier journal sur la configuration de votre ordinateur. Pour en enregistrer un, dans le menu principal, sélectionnez **Fichier** > **Enregistrer le journal**. Les journaux sont enregistrés au format XML. Par défaut,

les fichiers sont enregistrés dans le répertoire *%USERPROFILE%\Mes documents*, conformément à la convention de dénomination de fichier « SysInpsector-%COMPUTERNAME%-AAMMJJ-HHMM.XML ». Vous pouvez changer l'emplacement et le nom du fichier avant de l'enregistrer si vous le souhaitez.

Comment puis-je consulter le fichier journal d'ESET SysInspector ?

Pour consulter un fichier journal créé par ESET SysInspector, exécutez le programme et choisissez **Fichier** > **Ouvrir le journal** dans le menu principal. Vous pouvez également faire glisser les fichiers journaux et les déposer sur l'application ESET SysInspector. Si vous devez consulter fréquemment les fichiers journaux ESET SysInspector, il est conseillé de créer un raccourci vers le fichier SYSINSPECTOR.exe sur le Bureau ; vous pourrez ensuite faire glisser les fichiers et les déposer sur ce raccourci. Pour des raisons de sécurité, Windows Vista/7 peuvent désactiver la fonction glisser-déposer entre des fenêtres dont les autorisations diffèrent.

Existe-t-il une spécification pour le format de fichier journal ? Existe-t-il un kit de développement logiciel (SDK) ?

Pour l'instant, il n'existe ni spécifications pour le fichier journal ni SDK, car le programme est toujours au stade du développement. Après la sortie du programme, nous fournirons ces éléments sur la base des commentaires et des demandes des clients.

Comment ESET SysInspector évalue-t-il le risque que pose un objet en particulier ?

Dans la majorité des cas, ESET SysInspector attribue des niveaux de risque aux objets (fichiers, processus, clés de registre, etc.) sur la base d'une série de règles heuristiques qui examinent les caractéristiques de chaque objet, puis qui évaluent le potentiel d'activité malveillante. Cette analyse heuristique attribue aux objets un niveau de risque allant de 1 - OK (vert) à 9 - Risqué (rouge). Dans le volet de navigation gauche, la couleur des sections est définie par le niveau de risque le plus élevé d'un des objets qu'elles contiennent.

Un niveau de risque « 6 - Inconnu (rouge) » signifie-t-il que l'objet est dangereux ?

Les évaluations d'ESET SysInspector ne garantissent pas qu'un objet est malveillant. Cette réponse doit être apportée par l'expert en sécurité. ESET SysInspector a été développé pour fournir aux experts en sécurité une évaluation rapide afin qu'ils puissent identifier les objets d'un système qui devront faire l'objet d'un examen plus approfondi en cas de comportement étrange.

Pourquoi ESET SysInspector se connecte-t-il à Internet ?

À l'instar de nombreuses applications, ESET SysInspector possède un « certificat » avec signature numérique qui permet de garantir que le logiciel a bien été diffusé par ESET et qu'il n'a pas été modifié. Afin de vérifier le certificat, le système d'exploitation contacte une autorité de certification pour confirmer l'identité de l'éditeur de logiciels. Il s'agit d'un comportement normal pour tous les programmes avec signature numérique sous Microsoft Windows.

Qu'est-ce que la technologie Anti-Stealth ?

La technologie Anti-Stealth permet de détecter avec efficacité les rootkits.

Quand un système est attaqué par un code malveillant qui se comporte comme un rootkit, l'utlisateur risque de voir ses données endommagées ou volées. Sans outil spécial de lutte contre les rootkits, il est pratiquement impossible de les détecter.

Pourquoi y a-t-il parfois des fichiers marqués comme « Signé par MS » avec une valeur différente dans le champ « Nom de la société » ?

Lorsqu'ESET SysInspector tente d'identifier la signature numérique d'un fichier exécutable, il vérifie d'abord si une signature numérique est intégrée au fichier. Si c'est le cas, le fichier est validé avec ces informations. Si le fichier ne contient pas de signature numérique, ESI lance la recherche du fichier CAT correspondant (Catalogue de sécurité - *%systemroot%\system32\catroot*) qui contient des informations sur le fichier exécutable traité. Si le fichier CAT pertinent est trouvé, sa signature numérique est appliquée dans la procédure de validation du fichier exécutable.

Voilà pourquoi des fichiers sont parfois marqués « Signé par MS » mais ont un « Nom de la société » différent.

Exemple :

Windows 2000 comprend l'application HyperTerminal qui se trouve dans *C:\Program Files\Windows NT*. Le fichier exécutable principal de l'application n'a pas de signature numérique, mais ESET SysInspector l'indique comme étant un fichier signé par Microsoft. Ceci s'explique par une référence dans *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* qui pointe vers *C:\Program Files\Windows NT\hypertrm.exe* (le fichier exécutable principal de l'application HyperTerminal) et *sp4.cat* qui possède une signature numérique de Microsoft.

5.5.6 ESET SysInspector en tant que composant de ESET Smart Security

Pour ouvrir la section ESET SysInspector dans ESET Smart Security, cliquez sur **Outils** > **ESET SysInspector**. Le système de gestion disponible dans la fenêtre ESET SysInspector est semblable à celui des journaux d'analyse des ordinateurs ou des tâches planifiées. Toutes les opérations effectuées avec des instantanés système (création, affichage, comparaison, suppression et exportation) sont accessibles en un ou deux clics.

La fenêtre ESET SysInspector contient les informations élémentaires concernant les instantanés créés : heure de création, bref commentaire, nom de l'utilisateur auteur de l'instantané et statut de l'instantané.

Pour comparer, créer ou supprimer des instantanés, utilisez les boutons correspondants situés en dessous de la liste des instantanés dans la fenêtre ESET SysInspector. Ces options sont également disponibles dans le menu contextuel. Pour afficher l'instantané du système sélectionné, utilisez l'option **Afficher** du menu contextuel. Pour exporter l'instantané sélectionné dans un fichier, cliquez dessus avec le bouton droit de la souris et sélectionnez **Exporter...**

Voici la description détaillée des options disponibles :

- La fonctionnalité **Comparer** permet de comparer deux journaux. Elle est particulièrement adaptée si vous souhaitez effectuer le suivi des modifications entre le journal actuel et un ancien journal. Pour que cette option entre en vigueur, vous devez sélectionner deux instantanés à comparer.
- **Créer...** - Crée un enregistrement. Vous devez d'abord saisir un bref commentaire concernant l'enregistrement. Pour consulter le pourcentage de progression de la création de l'instantané en cours, consultez la colonne **État**. Tous les instantanés générés présentent l'état **Créé**.
- **Supprimer/Supprimer tout** - Supprime les entrées de la liste.
- **Exporter...** - Cette option enregistre l'entrée sélectionnée dans un fichier XML (également dans une version compressée).

5.6 ESET SysRescue

ESET SysRescue est un utilitaire qui vous permet de créer un disque d'amorçage contenant l'une des solutions de sécurité ESET Security ; cela peut être ESET NOD32 Antivirus, ESET Smart Security ou même l'un des produits orientés serveur. Le principal avantage d'ESET SysRescue réside dans le fait que la solution ESET Security est exécutée indépendamment du système d'exploitation hôte, tout en ayant un accès direct au disque et à l'ensemble du système de fichiers. Il est par conséquent possible de supprimer les infiltrations qui ne pourraient normalement pas être supprimées, par exemple lorsque le système d'exploitation est en cours d'exécution.

5.6.1 Configuration minimale requise

ESET SysRescue fonctionne dans l'environnement de préinstallation Microsoft Windows (Windows PE) version 2.x basé sur Windows Vista.

Windows PE faisant partie du kit d'installation automatisée de Windows (Windows AIK), ce kit doit être installé avant la création de ESET SysRescue (http://go.eset.eu/AIK). Windows PE prenant en charge la version 32 bits, le package d'installation de la solution ESET Security 32 bits doit être installé lors de la création de ESET SysRescue sur des systèmes 64 bits. ESET SysRescue prend en charge Windows AIK 1.1 et les versions ultérieures.

REMARQUE : La taille de Windows AIK étant supérieure à 1 Go, une connexion Internet à haut débit est nécessaire pour le télécharger dans de bonnes conditions.

ESET SysRescue est disponible dans les solutions ESET Security version 4.0 et ultérieures.

Systèmes d'exploitation pris en charge

- Windows 7
- Windows Vista
- Windows Vista Service Pack 1
- Windows Vista Service Pack 2
- Windows Server 2008
- Windows Server 2003 Service Pack 1 avec KB926044
- Windows Server 2003 Service Pack 2
- Windows XP Service Pack 2 avec KB926044
- Windows XP Service Pack 3

5.6.2 Procédure de création d'un CD de dépannage

Pour lancer l'assistant ESET SysRescue, cliquez sur **Démarrer** > **Programmes** > **ESET** > **ESET Smart Security** > **ESET SysRescue**.

Tout d'abord, l'Assistant vérifie si Windows AIK est installé et si un périphérique adapté pour la création du support d'amorçage est présent. Si Windows AIK n'est pas installé sur l'ordinateur (ou si l'installation est endommagée ou incorrecte), l'assistant vous propose de l'installer ou de saisir le chemin d'accès à votre dossier Windows AIK (http://go.eset.eu/AIK).

REMARQUE : La taille de Windows AIK étant supérieure à 1 Go, une connexion Internet à haut débit est nécessaire pour le télécharger dans de bonnes conditions.

Au cours de l'étape suivante, sélectionnez le support cible où ESET SysRescue sera stocké.

5.6.3 Sélection de la cible

Outre la sauvegarde sur un CD/DVD/périphérique USB, vous pouvez enregistrer ESET SysRescue dans un fichier ISO. Vous pouvez ensuite graver l'image ISO sur un CD/DVD, ou l'utiliser d'une autre manière (dans un environnement virtuel tel que VmWare ou Virtualbox par exemple).

Si vous choisissez le support cible USB, le démarrage peut ne pas fonctionner sur certains ordinateurs. Certaines versions du BIOS peuvent signaler des problèmes de communication entre le BIOS et le gestionnaire de démarrage (par exemple sous Windows Vista) et le démarrage s'arrête sur l'erreur suivante :

```
file : \boot\bcd
status : 0xc000000e
info : an error occurred while attemping to read the boot configuration data (info : une erreur s'est produi
```

Si ce message s'affiche, il est conseillé de sélectionner un CD au lieu du support USB.

5.6.4 Paramètres

Avant de commencer la création d'ESET SysRescue, l'assistant d'installation affiche les paramètres de compilation à la dernière étape de l'assistant ESET SysRescue. Pour les modifier, cliquez sur le bouton **Modifier...** Les options disponibles sont les suivantes :

- Dossiers
- ESET Antivirus
- Paramètres avancés
- Protocole Internet
- Périphérique USB d'amorçage (lorsque le périphérique USB de destination est sélectionné)
- Gravure (Lorsque le lecteur de CD/DVD de destination est sélectionné)

Le bouton **Créer** est inactif si aucun package d'installation MSI n'a été défini ou si aucune solution ESET Security n'est installée sur l'ordinateur. Pour sélectionner un package d'installation, cliquez sur le bouton **Modifier**, puis accédez à l'onglet **Antivirus ESET**. Si vous ne saisissez pas le nom d'utilisateur et le mot de passe (**Modifier** > **Antivirus ESET**), le bouton **Créer** est grisé.

5.6.4.1 Dossiers

Le **dossier temporaire** est un dossier de travail dans lequel sont stockés les fichiers nécessaires à la compilation d'ESET SysRescue.

Le **dossier ISO** est un dossier dans lequel est enregistré le fichier ISO après la compilation.

La liste dans cet onglet répertorie tous les disques de réseau locaux et mappés, ainsi que l'espace disponible. Si certains des dossiers sont stockés sur un lecteur ne disposant pas de l'espace suffisant, il est conseillé de sélectionner un autre lecteur avec plus d'espace disponible. Dans le cas contraire, la compilation pourrait s'arrêter prématurément en raison d'un manque d'espace sur le disque.

Applications externes : vous permet d'indiquer des programmes supplémentaires qui seront exécutés ou installés après l'amorçage depuis un support ESET SysRescue.

Inclure les applications externes : permet d'ajouter des programmes externes à la compilation ESET SysRescue.

Dossier sélectionné : dossier dans lequel se trouvent les programmes à ajouter au disque ESET SysRescue.

5.6.4.2 ESET Antivirus

Pour créer le CD ESET SysRescue, vous pouvez sélectionner deux sources de fichiers ESET à utiliser par le compilateur.

Dossier ESS/EAV - Fichiers déjà contenus dans le dossier dans lequel la solution ESET Security est installée sur l'ordinateur.

Fichier MSI : les fichiers contenus dans le programme d'installation MSI sont utilisés.

Vous pouvez ensuite choisir de mettre à jour l'emplacement des fichiers d'installation (.nup). L'option par défaut **Dossier ESS/EAV/Fichier MSI** doit normalement être sélectionnée. Dans certains cas, un **dossier de mise à jour** personnalisé peut être choisi, pour utiliser par exemple une version de base des signatures de virus ancienne ou récente.

Vous pouvez utiliser l'une des deux sources suivantes pour le nom d'utilisateur et le mot de passe :

ESS/EAV installé - Le nom d'utilisateur et le mot de passe sont copiés depuis la version installée de la solution ESET Security.

De l'utilisateur - Le nom d'utilisateur et le mot de passe saisis dans les zones de texte correspondantes sont utilisés.

REMARQUE : La solution ESET Security sur le CD ESET SysRescue est mise à jour soit via Internet, soit par l'intermédiaire de la solution ESET Security installée sur l'ordinateur où le CD ESET SysRescue est exécuté.

5.6.4.3 Paramètres avancés

L'onglet **Avancé** permet d'optimiser le CD ESET SysRescue en fonction de la quantité de mémoire disponible sur l'ordinateur. Sélectionnez **576 Mo et plus** pour écrire le contenu du CD dans la mémoire vive (RAM). Si vous choisissez **moins de 576 Mo**, l'accès au CD de récupération est permanent lorsque WinPE est en exécution.

Pilotes externes : cette section permet d'installer les pilotes de votre matériel (en général, de la carte réseau). Bien que WinPE repose sur Windows Vista PS1 qui prend en charge une large gamme de matériels, il arrive parfois que le matériel ne soit pas reconnu. Dans ce cas, un pilote doit être ajouté manuellement. L'installation du pilote dans la compilation ESET SysRescue peut s'effectuer de deux manières : manuellement (à l'aide du bouton **Ajouter**) et automatiquement (par l'intermédiaire du bouton **Recherche auto**). En cas d'inclusion manuelle, vous devez choisir le chemin d'accès au fichier .inf correspondant (le fichier *.sys applicable doit se trouver également dans le dossier). En cas d'installation automatique, le pilote est détecté automatiquement dans le système d'exploitation de l'ordinateur. Il est conseillé d'utiliser l'inclusion automatique uniquement si ESET SysRescue est utilisé sur un ordinateur qui dispose de la même carte réseau que l'ordinateur sur lequel le CD ESET SysRescue a été créé. Lors de la création d'ESET SysRescue, le pilote est installé dans la compilation, ce qui évite à l'utilisateur d'avoir à le rechercher ultérieurement.

5.6.4.4 Protocole Internet

Cette section permet de configurer les informations réseau de base et les connexions prédéfinies après ESET SysRescue.

Sélectionnez **Adresse IP privée automatique** pour obtenir automatiquement l'adresse IP depuis le serveur DHCP (Dynamic Host Configuration Protocol).

Cette connexion réseau peut également utiliser une adresse IP spécifiée manuellement (appelée également adresse IP statique). Sélectionnez **Personnalisé** pour configurer les paramètres IP appropriés. Si vous sélectionnez cette option, vous devez indiquer une **adresse IP** et, pour les connexions au réseau LAN et les connexions Internet haut débit, un **masque de sous-réseau**. Dans les zones **Serveur DNS préféré** et **Serveur DNS de rechange**, saisissez les adresses des serveurs DNS principal et secondaire.

5.6.4.5 Périphérique USB d'amorçage

Si vous avez choisi le périphérique USB en tant que support cible, vous pouvez choisir l'un des supports USB disponibles dans l'onglet **Périphérique USB d'amorçage** (si plusieurs périphériques USB existent).

Sélectionnez le **périphérique** sur lequel ESET SysRescue doit être installé.

Avertissement : le périphérique USB sélectionné est formaté lors de la création d'ESET SysRescue. Toutes les données du périphérique sont supprimées.

Si vous choisissez l'option de **format rapide**, le formatage supprime tous les fichiers de la partition, mais ne recherche pas les secteurs défectueux du disque. Utilisez cette option si votre périphérique USB a été formaté précédemment et que vous êtes certain qu'il n'est pas endommagé.

5.6.4.6 Graver

Si vous avez choisi le support cible CD/DVD, vous pouvez définir les paramètres de gravure complémentaires dans l'onglet **Graver**.

Supprimer fichier ISO : cochez cette case pour supprimer les fichiers ISO après la création du CD ESET SysRescue.

Suppression activée : permet de choisir entre la suppression rapide et la suppression complète.

Graveur : choisissez le lecteur à utiliser pour la gravure.

Avertissement : il s'agit de l'option par défaut. En cas d'utilisation d'un CD/DVD réinscriptible, toutes les données stockées sur le CD/DVD sont supprimées.

La section Support contient des informations sur le support dans le lecteur de CD/DVD.

Vitesse de gravure : sélectionnez la vitesse souhaitée dans le menu déroulant. Les capacités du périphérique de gravure et le type de CD/DVD utilisé doivent être pris en compte lors de la sélection de la vitesse de gravure.

5.6.5 Travailler avec ESET SysRescue

Pour que le CD/DVD/USB de récupération fonctionne efficacement, l'ordinateur doit être démarré depuis le support d'amorçage ESET SysRescue. La priorité d'amorçage peut être modifiée dans le BIOS. Vous pouvez également utiliser le menu d'amorçage au démarrage de l'ordinateur (généralement à l'aide de l'une des touches F9 à F12, en fonction de la version de la carte mère ou du BIOS).

Une fois l'amorçage depuis le support d'amorçage terminé, la solution ESET Security démarre. Comme ESET SysRescue n'est utilisé que dans des situations spécifiques, certains modules de protection et fonctionnalités de programme présents dans la version standard d'ESET Security ne sont pas nécessaires ; leur liste est limitée à l'**analyse de l'ordinateur**, à la **mise à jour** et à certaines sections de la **configuration**. ESET SysRescue peut mettre à jour la base des signatures de virus. C'est la principale fonctionnalité de cette application et nous vous recommandons d'effectuer cette mise à jour avant de lancer l'analyse de l'ordinateur.

5.6.5.1 Travailler avec ESET SysRescue

Supposons que des ordinateurs du réseau aient été infectés par un virus modifiant les fichiers exécutables (.exe). La solution ESET Security est capable de nettoyer tous les fichiers infectés, à l'exception d'*explorer.exe* qui ne peut pas être nettoyé, même en mode sans échec. Cela s'explique par le fait que le fichier *explorer.exe*, l'un des processus Windows essentiel, est lui-même lancé en mode sans échec. La solution ESET Security n'est pas en mesure d'intervenir sur ce fichier et ce dernier reste infecté.

Dans ce type de scénario, vous pouvez utiliser ESET SysRescue pour résoudre le problème. ESET SysRescue ne requiert aucun composant du système d'exploitation hôte et peut traiter (nettoyer, supprimer) n'importe quel fichier du disque.

6. Glossaire

6.1 Types d'infiltrations

Une infiltration est un élément de logiciel malveillant qui tente de s'introduire dans l'ordinateur d'un utilisateur et/ou de l'endommager.

6.1.1 Virus

Un virus d'ordinateur est un fragment de code malveillant qui est ajouté à des fichiers qui sont sur votre ordinateur. Les virus informatiques sont comparables aux virus biologiques parce qu'ils utilisent des techniques similaires pour se propager d'un ordinateur à l'autre. Le terme « virus » est quant à lui souvent utilisé de manière abusive pour décrire tout type de menace. On tend à le remplacer progressivement par le terme « logiciel malveillant » ou « malware » en anglais.

Les virus informatiques attaquent principalement les fichiers et documents exécutables. En bref, un virus informatique fonctionne de la manière suivante : après l'exécution d'un fichier infecté, le code malveillant est appelé et exécuté avant l'exécution de l'application originale. Un virus peut infecter tous les fichiers pour lesquels l'utilisateur a des droits d'écriture.

Les virus peuvent varier en fonction de leur gravité et de leur cible. Certains sont extrêmement dangereux parce qu'ils ont la capacité de supprimer délibérément des fichiers du disque dur. D'autres, en revanche, ne causent pas de réels dommages : ils ne servent qu'à gêner l'utilisateur et à démontrer les compétences techniques de leurs auteurs.

Si votre ordinateur est infecté par un virus et qu'il est impossible de le nettoyer, soumettez-le au laboratoire d'ESET pour examen. Dans certains cas, les fichiers infectés peuvent avoir subi des modifications telles, qu'il est impossible de les nettoyer. Il faut alors les remplacer par une copie propre.

6.1.2 Vers

Un ver est un programme contenant un code malveillant qui attaque les ordinateurs hôtes et se propage via un réseau. La différence fondamentale entre les virus et les vers réside dans le fait que les vers ont la capacité de se propager par eux-mêmes. Ils ne dépendent pas des fichiers hôtes (ou des secteurs d'amorçage). Les vers se propagent par l'intermédiaire des adresses de messagerie de votre liste de contacts ou exploitent les vulnérabilités de sécurité des applications réseau.

Les vers sont ainsi susceptibles de vivre beaucoup plus longtemps que les virus. Par le biais d'Internet, ils peuvent se propager à travers le monde en quelques heures seulement et parfois en quelques minutes. Leur capacité à se répliquer indépendamment et rapidement les rend plus dangereux que les autres types de programmes malveillants.

Un ver activé dans un système peut être à l'origine de plusieurs dérèglements : il peut supprimer des fichiers, dégrader les performances du système ou même désactiver certains programmes. Par nature, il peut servir de « moyen de transport » à d'autres types d'infiltrations.

Si votre ordinateur est infecté par un ver, il est recommandé de supprimer les fichiers infectés, car ils contiennent probablement du code malveillant.

6.1.3 Chevaux de Troie

Les chevaux de Troie ont été définis comme une catégorie de menaces dont la particularité est de se présenter comme des programmes utiles pour duper ensuite les utilisateurs qui acceptent de les exécuter.

La catégorie étant très vaste, elle est souvent divisée en plusieurs sous-catégories :

- **Téléchargeur** - Programmes malveillants qui sont en mesure de télécharger d'autres menaces sur Internet.
- **Dropper** - Programmes malveillants qui sont en mesure de déposer d'autres types de logiciels malveillants sur des ordinateurs infectés.
- **Backdoor** - Programmes malveillants qui communiquent avec des attaquants distants, leur permettant d'accéder à l'ordinateur et d'en prendre le contrôle.
- **Keylogger** - Programme qui enregistre chaque touche sur laquelle tape l'utilisateur et envoie les informations aux pirates.
- **Composeur** - Programmes malveillants destinés à se connecter à des numéros surtaxés au lieu du fournisseur de services Internet de l'utilisateur. Il est presque impossible qu'un utilisateur remarque la création d'une nouvelle connexion. Les composeurs ne peuvent porter préjudice qu'aux utilisateurs ayant des modems par ligne commutée, qui sont de moins en moins utilisés.

Si un fichier est identifié comme cheval de Troie sur votre ordinateur, il est recommandé de le supprimer, car il est fort probable qu'il ne contienne rien d'autre que du code malveillant.

6.1.4 Rootkits

Les rootkits sont des programmes malveillants qui procurent aux pirates un accès illimité à un système tout en dissimulant leur présence. Après avoir accédé au système (généralement en exploitant une faille), les rootkits utilisent des fonctions du système d'exploitation pour se protéger des logiciels antivirus : ils dissimulent des processus, des fichiers et des données de la base de registre Windows. Pour cette raison, il est presque impossible de les détecter à l'aide des techniques de test ordinaires.

Il existe deux niveaux de détection permettant d'éviter les rootkits :

1. Lorsqu'ils essaient d'accéder au système. Ils ne sont pas encore installés et donc inactifs. La plupart des antivirus sont en mesure d'éliminer les rootkits à ce niveau (en supposant qu'ils détectent effectivement les fichiers comme infectés).
2. Lorsqu'ils sont inaccessibles aux tests habituels. Les utilisateurs ESET Smart Security bénéficient de la technologie Anti-Stealth qui permet de détecter et d'éliminer les rootkits en activité.

6.1.5 Logiciels publicitaires

Le terme anglais « adware » désigne les logiciels soutenus par la publicité. Les programmes qui affichent des publicités entrent donc dans cette catégorie. Les logiciels publicitaires ouvrent généralement une nouvelle fenêtre contextuelle automatiquement dans un navigateur Internet. Cette fenêtre contient de la publicité ou modifie la page de démarrage du navigateur. Ils sont généralement associés à des programmes gratuits et permettent aux développeurs de couvrir les frais de développement de leurs applications (souvent utiles).

Les logiciels publicitaires en tant que tels ne sont pas dangereux ; ils dérangent simplement les utilisateurs en affichant des publicités. Le danger réside dans le fait qu'ils peuvent également avoir des fonctions d'espionnage (comme les logiciels espions).

Si vous décidez d'utiliser un logiciel gratuit, soyez particulièrement attentif au programme d'installation. La plupart des programmes d'installation vous avertissent en effet qu'ils installent également un programme publicitaire. Dans la plupart des cas, vous pourrez désactiver cette installation supplémentaire et installer le programme sans logiciel publicitaire.

Certains programmes refusent de s'installer sans leur logiciel publicitaire ou voient leurs fonctionnalités limitées. Cela signifie que les logiciels publicitaires accèdent souvent au système de manière « légale », dans la mesure où les utilisateurs l'ont accepté. Dans ce cas, il est préférable de procéder avec prudence. Si un logiciel publicitaire est détecté sur votre ordinateur, il est conseillé de le supprimer, car il est fort probable qu'il contienne du code malveillant.

6.1.6 Logiciels espions

Cette catégorie englobe toutes les applications qui envoient des informations confidentielles sans le consentement des utilisateurs et à leur insu. Les logiciels espions utilisent des fonctions de traçage pour envoyer diverses données statistiques telles que la liste des sites Web visités, les adresses e-mail de la liste de contacts de l'utilisateur ou la liste des touches du clavier utilisées.

Les auteurs de ces logiciels espions affirment que ces techniques ont pour but d'en savoir plus sur les besoins et intérêts des utilisateurs afin de mieux cibler les offres publicitaires. Le problème est qu'il n'y a pas de distinction claire entre les applications utiles et les applications malveillantes, et que personne ne peut garantir que les informations récupérées ne sont pas utilisées à des fins frauduleuses. Les données récupérées par les logiciels espions peuvent être des codes de sécurité, des codes secrets, des numéros de compte bancaire, etc. Les logiciels espions sont souvent intégrés aux versions gratuites d'un programme dans le but de générer des gains ou d'inciter à l'achat du logiciel. Les utilisateurs sont souvent informés de la présence d'un logiciel espion au cours de l'installation d'un programme qui vise à les inciter à acquérir la version payante qui en est dépourvue.

Parmi les produits logiciels gratuits bien connus qui contiennent des logiciels espions, on trouve les applications clients de réseaux P2P (poste à poste). Spyfalcon ou Spy Sheriff (et beaucoup d'autres) appartiennent à une sous-catégorie spécifique de logiciels espions : ils semblent être des programmes antispyware alors qu'ils sont en réalité eux-mêmes des logiciels espions.

Si un fichier est détecté comme logiciel espion sur votre ordinateur, il est préférable de le supprimer, car il est fort probable qu'il contienne du code malveillant.

6.1.7 Applications potentiellement dangereuses

Il existe de nombreux programmes authentiques qui permettent de simplifier l'administration des ordinateurs en réseau. Toutefois, s'ils tombent entre de mauvaises mains, ces programmes sont susceptibles d'être utilisés à des fins malveillantes. ESET Smart Security permet de détecter ces menaces.

Applications potentiellement dangereuses est la classification utilisée pour les logiciels commerciaux légitimes. Cette classification comprend les programmes d'accès à distance, les applications de résolution de mot de passe ou les keyloggers (programmes qui enregistrent chaque frappe au clavier de l'utilisateur).

Si vous découvrez qu'une application potentiellement dangereuse est présente et fonctionne sur votre ordinateur (sans que vous ne l'ayez installée), consultez l'administrateur réseau ou supprimez l'application.

6.1.8 Applications potentiellement indésirables

Les **applications potentiellement indésirables** ne sont pas nécessairement malveillantes, mais elles sont susceptibles d'affecter les performances de votre ordinateur. Ces applications sont habituellement installées après consentement. Si elles sont présentes sur votre ordinateur, votre système se comporte différemment (par rapport à son état avant l'installation). Voici les changements les plus significatifs :

- affichage de nouvelles fenêtres (fenêtres contextuelles, publicités) ;
- activation et exécution de processus cachés ;
- augmentation de l'utilisation des ressources système ;
- modification des résultats de recherche ;
- communication de l'application avec des serveurs distants.

6.2 Types d'attaques distantes

Il existe diverses techniques permettant à des pirates de mettre en péril des systèmes distants. Elles se divisent en plusieurs catégories.

6.2.1 Attaques DoS

L'attaque DoS, ou attaque par *déni de service*, vise à rendre un ordinateur ou un réseau indisponible pour ses utilisateurs. La communication entre les utilisateurs affectés est obstruée et ne peut plus continuer normalement. Les ordinateurs qui ont subi une attaque DoS doivent généralement redémarrer pour fonctionner correctement.

Dans la plupart des cas, le déni de service cible les serveurs Web et cherche à les rendre inutilisables pendant un certain temps.

6.2.2 Empoisonnement DNS

En utilisant l'empoisonnement DNS, les pirates peuvent faire croire au serveur DNS de tout ordinateur que les fausses données qui leur sont transmises sont légitimes et authentiques. Ces fausses informations sont ensuite mises en cache pendant un certain temps, ce qui permet aux attaquants de réécrire les réponses DNS des adresses IP. De cette manière, les utilisateurs qui tentent d'accéder à des sites internet téléchargeront des virus ou des vers au lieu du contenu original de ces sites.

6.2.3 Attaques de vers

Un ver est un programme contenant un code malveillant qui attaque les ordinateurs hôtes et se propage via un réseau. Les vers de réseau exploitent les failles de sécurité de diverses applications. Par le biais d'Internet, ils peuvent se propager à travers le monde en quelques heures seulement et parfois même en quelques minutes.

La plupart des attaques de ver (Sasser, SqlSlammer) peuvent être évitées en utilisant les paramètres de sécurité par défaut du pare-feu ou en bloquant les ports non protégés et non utilisés. Il est également essentiel d'appliquer les derniers correctifs de sécurité au système d'exploitation.

6.2.4 Balayage de ports

Le balayage de ports permet de déterminer les ports ouverts sur un ordinateur ou un hôte du réseau. Le logiciel utilisé à cette fin s'appelle scanneur de ports.

Le port d'un ordinateur est un point virtuel qui traite les données entrantes et sortantes. C'est un point crucial pour la sécurité. Sur un réseau de grande taille, les informations collectées par le scanneur de ports peuvent permettre d'identifier les failles potentielles. Cette utilisation est bien sûr tout à fait légale.

Néanmoins, le balayage de ports est souvent utilisé par les pirates qui tentent de compromettre la sécurité. Ils envoient d'abord des paquets à chaque port. En fonction du type de réponse, ils parviennent à déterminer les ports qui sont utilisés. Si le balayage lui-même ne cause aucun dommage, cette activité peut révéler les failles potentielles et permettre aux pirates de prendre le contrôle d'ordinateurs distants.

Nous conseillons aux administrateurs du réseau de bloquer tous les ports non utilisés et de protéger ceux qui sont utilisés des accès non autorisés.

6.2.5 Désynchronisation TCP

La désynchronisation TCP est une technique utilisée pour les détournements de session TCP (TCP Hijacking). Elle est déclenchée par un processus dans lequel le numéro séquentiel de paquets entrants diffère du numéro attendu. Les paquets dont le numéro séquentiel est différent de celui attendu sont rejetés (ou enregistrés dans la mémoire tampon, s'ils sont présents dans la fenêtre de communication active).

Lorsqu'il y a désynchronisation, les deux extrémités de la communication refusent les paquets reçus. C'est ici que les pirates peuvent intervenir à distance pour infiltrer et fournir des paquets dont le numéro séquentiel est correct. Les pirates peuvent même manipuler ou modifier la communication.

Les détournements de session TCP visent à interrompre les communications serveur-client ou les communications poste à poste. De nombreuses attaques peuvent être évitées par l'authentification de chaque segment TCP. Il est également conseillé d'utiliser les configurations recommandées pour vos périphériques réseau.

6.2.6 Relais SMB

SMBRelay et SMBRelay2 sont des programmes spéciaux permettant de mener une attaque contre des ordinateurs distants. Les programmes tirent parti du protocole de partage de fichiers SMB (Server Message Block) situé sur NetBIOS. Lorsqu'un utilisateur partage des dossiers ou répertoires sur un réseau local, il utilise très probablement ce protocole de partage de fichiers.

Au cours des communications sur le réseau local, les empreintes numériques des mots de passe sont échangées.

SMBRelay reçoit une connexion sur les ports UDP 139 et 445, relaie les paquets échangés par le client et le serveur, et les modifie. Après connexion et authentification, le client est déconnecté. SMBRelay crée une nouvelle adresse virtuelle IP, à laquelle il est possible d'accéder à l'aide de la commande "net use \\192.168.1.1". L'adresse peut ensuite être utilisée par n'importe quelle fonction de réseau de Windows. SMBRelay relaie les communications du protocole SMB, sauf la négociation et l'authentification. Les pirates peuvent utiliser l'adresse IP tant que l'ordinateur client est connecté.

SMBRelay2 fonctionne selon le même principe que SMBRelay, si ce n'est qu'il utilise les noms NetBIOS plutôt que les adresses IP. Tous deux peuvent mener des attaques dites de « l'homme du milieu » (man-in-the-middle). Ces attaques permettent à des pirates de lire, d'insérer des données et de modifier à distance les messages échangés entre deux points de communication sans être remarqués. Les ordinateurs exposés à ce type d'attaque arrêtent souvent de répondre ou redémarrent de manière impromptue.

Pour éviter de telles attaques, nous vous recommandons d'utiliser des mots de passe ou des clés d'authentification.

6.2.7 Attaques par protocole ICMP

L'ICMP (Internet Control Message Protocol) est un protocole Internet très utilisé. Il est surtout utilisé par les ordinateurs en réseau pour envoyer différents messages d'erreur.

Les attaquants distants tentent d'exploiter la faiblesse du protocole ICMP. Le protocole ICMP est conçu pour les communications à sens unique n'exigeant pas d'authentification. Ceci permet aux attaquants distants de déclencher des « attaques DoS » (Denial of Service (déni de service)). Il s'agit d'attaques qui permettent aux personnes non autorisées d'accéder à des paquets entrants et sortants.

Le Ping Flood (inondation par flux de ping), l'ICMP_ECHO flood et le smurf sont des exemples typiques d'attaques ICMP. Les ordinateurs exposés aux attaques ICMP sont considérablement ralentis (ceci est valable pour toutes les applications qui utilisent Internet) et ont des problèmes de connexion Internet.

6.3 Courrier électronique

Le courrier électronique est une forme de communication moderne qui offre beaucoup d'avantages. Adaptable, rapide et direct, il a joué un rôle crucial dans l'expansion d'Internet au début des années 90.

Malheureusement, le grand anonymat des courriers électroniques et Internet a laissé libre champ aux activités illégales telles que le « spamming » (le fait d'envoyer des messages indésirables à un grand nombre de personnes). Les courriers indésirables comprennent les publicités indésirables, les canulars et les logiciels malveillants. Les désagréments et le danger augmentent, car l'envoi de tels messages ne coûte rien et les auteurs de courrier indésirable disposent de nombreux outils qui leur permettent de se procurer facilement de nouvelles adresses de messagerie. Par ailleurs, le volume et la variété du courrier indésirable ne facilitent pas la réglementation. Plus vous utilisez votre adresse de messagerie, plus vous augmentez la possibilité d'aboutir dans un moteur de base de données de courrier indésirable. Voici quelques conseils de prévention :

- Évitez de publier votre adresse de messagerie sur Internet.
- Ne donnez votre adresse de messagerie qu'à des personnes fiables.
- Évitez d'utiliser des pseudonymes communs : un pseudonyme compliqué est moins susceptible d'être traqué.
- Ne répondez pas au courrier indésirable qui est arrivé dans votre boîte de réception.
- Faites attention lorsque vous remplissez des formulaires sur Internet : soyez particulièrement attentif aux options du type « Oui, je voudrais recevoir des informations concernant... ».
- Utilisez des adresses de messagerie « spécialisées », par exemple une adresse pour votre travail, une autre pour communiquer avec vos amis, etc.
- Changez vos adresses de messagerie de temps en temps.
- Utilisez une solution antispam.

6.3.1 Publicités

La publicité via Internet est une des formes de publicité les plus en vogue. D'un point de vue marketing, la publicité présente plusieurs avantages : ses coûts sont minimes, elle est très directe et les messages sont transmis presque immédiatement. De nombreuses entreprises utilisent des outils de marketing par courrier électronique pour communiquer de manière efficace avec leurs clients et prospects.

Ce mode de publicité est légitime, car vous pourriez être intéressé par la réception d'informations commerciales sur certains produits. Toutefois, de nombreuses entreprises envoient des masses de messages commerciaux non sollicités. La publicité par e-mail dépasse alors les limites et devient du courrier indésirable, ou spam.

La quantité de messages publicitaires non sollicités est devenue un réel problème, car elle ne montre aucun signe de ralentissement. Les auteurs de messages non sollicités tentent souvent de déguiser le courrier indésirable sous des dehors de messages légitimes.

6.3.2 Canulars

Un canular (ou hoax) est un message propagé sur Internet. Il est envoyé généralement avec le courrier et parfois par des outils de communication tels que ICQ et Skype. Le message est souvent une blague ou une légende urbaine.

Les canulars essaient de provoquer chez les destinataires de la peur, de l'incertitude et du doute, les amenant à croire qu'un « virus indétectable » supprime tous les fichiers et récupère les mots de passe, ou effectue une activité nuisible sur leur système.

Certains canulars demandent aux destinataires de transmettre des messages à leurs contacts, ce qui a pour conséquence de propager les canulars. Même les téléphones portables reçoivent des canulars et des demandes d'aide (des personnes proposant par exemple de vous envoyer de l'argent depuis l'étranger). Il est souvent impossible de déterminer l'intention du créateur.

Si un message vous demande de le faire suivre à toutes vos connaissances, il peut très bien s'agir d'un canular. Sur Internet, de nombreux sites spécialisés peuvent vérifier la légitimité d'un courrier. Avant de retransmettre un message que vous soupçonnez d'être un canular, faites d'abord une recherche sur Internet à son sujet.

6.3.3 Hameçonnage

Le terme d'hameçonnage (phishing en anglais) désigne une activité frauduleuse utilisant des techniques de piratage psychologique qui consistent à manipuler les utilisateurs pour obtenir des informations confidentielles. Son but est d'accéder à des données sensibles, telles que numéros de comptes bancaires, codes secrets, etc.

La technique consiste généralement à envoyer un message électronique en se faisant passer pour une personne ou une entreprise digne de confiance (institution financière, compagnie d'assurance par exemple). Le message peut sembler tout à fait authentique et contenir des graphiques et contenus qui proviennent véritablement de la source dont il se réclame. Vous êtes invité à entrer, sous divers prétextes (vérification de données, opérations financières), certaines de vos données personnelles : numéros de compte en banque ou noms d'utilisateur et mots de passe. Toutes ces données, si elles sont soumises, peuvent facilement être volées et utilisées à des fins illégales.

Les banques, compagnies d'assurance et autres sociétés légales ne demandent jamais de noms d'utilisateur et de mots de passe dans un message non sollicité.

6.3.4 Reconnaissance du courrier indésirable

Généralement, peu d'indicateurs contribuent à identifier le courrier indésirable (messages non sollicités) dans une boîte à lettres. Si un message remplit au moins l'un des critères suivants, il s'agit probablement de courrier indésirable.

- L'adresse de l'expéditeur ne figure pas dans la liste de vos contacts.
- Le contenu du message concerne une grosse somme d'argent qui vous est offerte. Pour toucher cette somme, vous devez néanmoins fournir au préalable une petite somme.
- Vous devez entrer, sous divers prétextes (vérification de données, opérations financières), certaines de vos données personnelles : numéros de compte en banque ou noms d'utilisateur et mots de passe.
- Le message est écrit dans une langue étrangère.
- Le message vous demande d'acheter un produit qui ne vous intéresse pas. Si vous décidez d'acheter le produit, vérifiez que l'expéditeur du message est un vendeur sérieux (consultez le fabricant original du produit).
- Quelques mots sont mal écrits pour pouvoir passer à travers le filtre de courrier indésirable. Par exemple, « vaigra » au lieu de « viagra », etc.

6.3.4.1 Règles

Dans le contexte des solutions de protection antispam et des clients de messagerie, les règles sont des outils permettant de manipuler les fonctions de messagerie. Elles se composent de deux parties logiques :

1. la condition (par exemple, un message entrant provenant d'une certaine adresse) ;
2. l'action (par exemple, la suppression du message ou son déplacement vers un dossier spécifique).

Le nombre de règles et leurs combinaisons varient en fonction de la solution de protection antispam. Ces règles servent de protection antispam (messages non sollicités). Exemples caractéristiques :

- 1. Condition : un message entrant contient des mots habituellement utilisés dans le courrier indésirable.
  2. Action : supprimer le message.

- 1. Condition : un message entrant contient une pièce jointe comportant l'extension .exe.
  2. Action : supprimer la pièce jointe et livrer le message dans la boîte aux lettres.

- 1. Condition : un message entrant arrive de votre employeur.
  2. Action : déplacer le message dans le dossier Travail.

Nous vous recommandons d'utiliser une combinaison de règles des programmes de programme antispam afin de faciliter l'administration et d'améliorer le filtrage du courrier indésirable.

6.3.4.2 Liste blanche

En général, une liste blanche est une liste de personnes ou d'éléments qui ont été acceptés ou ont obtenu une autorisation d'accès. Le terme « liste blanche de messagerie » définit la liste de contacts dont l'utilisateur souhaite recevoir les messages. Ces listes blanches sont basées sur des mots-clés recherchés dans une adresse électronique, des noms de domaines ou des adresses IP.

Si une liste blanche fonctionne en « mode exclusif », les messages de toutes les autres adresses, domaines ou adresses IP sont écartés. Si elle fonctionne en mode non exclusif, ces messages ne sont pas supprimés, mais filtrés d'une autre façon.

Une liste blanche fonctionne sur le principe opposé de la liste noire. Les listes blanches sont relativement faciles à maintenir, plus que les listes noires. Pour un meilleur filtrage du courrier indésirable, nous vous recommandons d'utiliser des listes blanches et des listes noires.

6.3.4.3 Liste noire

En général, une liste noire répertorie les personnes ou les éléments non acceptés ou interdits. Dans le monde virtuel, c'est une technique qui permet d'accepter des messages de tous les utilisateurs qui ne figurent pas sur cette liste.

Il existe deux types de listes noires : les listes créées par les utilisateurs dans l'application de protection antispam et les listes professionnelles mises à jour régulièrement. Ces dernières sont créées par des institutions spécialisées et sont disponibles sur Internet.

Il est essentiel d'utiliser les listes noires pour bloquer le courrier indésirable, mais elles sont très difficiles à tenir à jour, car de nouveaux éléments à bloquer apparaissent tous les jours. Nous recommandons d'utiliser à la fois une liste blanche et une liste noire pour mieux filtrer le courrier indésirable.

6.3.4.4 Contrôle côté serveur

Le contrôle côté serveur est une technique permettant d'identifier le courrier indésirable de masse d'après le nombre de messages reçus et les réactions des utilisateurs. Chaque message laisse une empreinte numérique unique en fonction de son contenu. Le numéro d'identification unique ne donne aucune information sur le contenu du message. Deux messages identiques ont une empreinte identique, tandis que des messages différents ont une empreinte différente.

Si un message est marqué comme courrier indésirable, son empreinte est envoyée au serveur. Si le serveur reçoit plusieurs empreintes identiques (correspondant à un certain message de courrier indésirable), cette empreinte est stockée dans la base des empreintes de courrier indésirable. Lorsqu'il analyse des messages entrants, le programme envoie les empreintes de ces messages au serveur. Le serveur renvoie des informations indiquant les empreintes qui correspondent à des messages déjà identifiés comme courrier indésirable par d'autres utilisateurs.